RouteFinder™ VPN

Internet Security Appliance

RF760/660/600VPN

Internet Security Appliance

User Guide

MultiTech® Systems

User Guide

RouteFinder RF760/660/600VPN
S000323D Revision D

Record of Revisions

Revision	Date	Description
A	01/30/04	First release for the RF760VPN. The guide combines the RF600VPN and the RF660VPN user information.
B	11/01/04 & 01/25/05	New software – version 3.20 and New software – version 3.21. POP3 Proxy new. New Rescue Kernel section.
C	04/19/05	New software – Version 3.23 (one new field on the SMTP SPAM screen and one new field on the Packet Filters > Advanced screen).
D	11/22/05	New software – Version 3.25. A System Scheduler was added to Administration. A User Authentication section was added to the Proxy > HTTP Proxy screen. A Remote SMTP Virus Quarantine section was added to Proxy > SMTP Proxy. Maximum Mail Size Allowed and Message Filtering added to Proxy >SMTP Proxy > SMTP SPAM Filtering. Remote POP3 Virus Protection section was added to Proxy > POP3 Proxy. A Message Filtering section was added to Proxy > POP3 Proxy > POP3SPAM Filtering. Adaptive Message Database Backup was added to the Tracking > Backup screen. The screen for Statistics & Logs > HTTP Access has been enhanced. Hardware change: new compact flash.

Patents

This device is covered by one or more of the following U.S. Patent Numbers: 6,219,708; 5,301,274; 5,309,562; 5,355,365; 5,355,653; 5,452,289; 5,453.986.
The modem is covered by one or more of the following U.S. Patent Numbers: 6,031,867; 6,012,113; 6,009,082; 5,905,794; 5,864,560; 5,815,567; 5,815,503; 5,812,534; 5,809,068; 5,790,532; 5,764,628; 5,764,627; 5,754,589; D394,250; 5,724,356; 5,673,268; 5,673,257; 5,644,594; 5,628,030; 5,619,508; 5,617,423; 5,600,649; 5,592,586; 5,577,041; 5,574,725; D374,222; 5,559,793; 5,546,448; 5,546,395; 5,535,204; 5,500,859; 5,471,470; 5,463,616; 5,453,986; 5,452,289; 5,450,425; D361,764; D355,658; D355,653; D353,598; D353,144; 5,355,365; 5,309,562; 5,301,274 Other Patents Pending

Trademarks

Trademarks of Multi-Tech Systems, Inc.: Multi-Tech, the Multi-Tech logo, and RouteFinder.
Windows is a registered trademark of Microsoft Corporation in the United States and other countries.
Kaspersky Anti-Virus engine copyright by Kaspersky Labs. Surfcontrol is the registered product of Surfcontrol PLC.
All products or technologies are the trademarks or registered trademarks of their respective holders.

Technical Support

Country	By Email	By Phone
France:	support@multitech.fr	(33) 1-64 61 09 81
India:	support@multitechindia.com	91 (124) 6340778
U.K.:	support@multitech.co.uk	(44) 118 959 7774
U.S. and Canada:	support@multitech.com	(800) 972-2439
Rest of the World:	support@multitech.com	(763) 717-5863

World Headquarters

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(763) 785-3500 or (800) 328-9717
Fax 763-785-9874
Internet Address: http://www.multitech.com

Contents

Chapter 1 – Product Description, Features, and Overview

Your Multi-Tech Systems, Inc. RouteFinder Internet security appliance is an integrated VPN gateway/firewall designed to maximize network security without compromising network performance. It uses data encryption, user authentication, and the Internet to securely connect telecommuters, remote offices, customers, and suppliers to the corporate office while avoiding the cost of private leased lines or dial-up charges.

Product Description

All three RouteFinder models provide advanced network firewall (Stateful Packet Inspection and NAT), application firewall (DMZ, proxies, filter, optional email anti-virus protection), VPN gateway (IPSec, PPTP, 3DES, authentication), and full router capabilities. Their Ethernet ports provide connectivity to your network, to the Internet access via router, DSL, cable or dedicated line, and to the DMZ.

The RouteFinder's DMZ port permits connecting of Voice over IP gateways, like MultiVOIPs, and public servers such as email and Web to be safely connected. And its full-featured router hardware allows the entire network to share an Internet link by connecting to an existing cable modem, DSL modem, or router.

An optional email anti-virus update product offered by Multi-Tech with your RouteFinder purchase includes protection against new virus types and security gaps with automatically transferred updates.

The browser-based interface eases VPN configuration and management. The VPN functionality is based on the IPSec and PPTP protocols and uses Triple DES 168-bit encryption to ensure that your information remains private. In addition, the RF760/660VPN includes firewall security utilizing Stateful Packet Inspection and optional email anti-virus protection.

The RouteFinder VPNs can be used on the desktop or mounted in racks.

Features

- Supports IPSec and PPTP VPN tunneling
- Utilizes 168-bit Triple Data Encryption Standard (3DES)
- Built-in Stateful Packet Inspection firewall with Network Address Translation (NAT)
- Encapsulating Security Protocol (ESP)
- Authentication Header (AH)
- Internet Key Exchange (IKE), with support of Diffie-Hellman Group 2
- Authentication Algorithm: HMAC-MD5 and HMAC-SHA1
- Authentication using shared secrets, RSA digital signatures, and X.509 certificates
- Perfect Forward Secrecy
- Key exchanges using Internet PKIs (Public Key Infrastructure)
- Free one-year content filtering subscription
- Automatic dial-backup with built-in modem (RF760VPN and RF660VPN)
- Automatic system updates to protect your network against the latest threats
- Application layer security using SMTP, POP3, HTTP, DNS and SOCKS proxies
- Secure local or remote management using HTTP, HTTPS or SSH
- Reporting function provides valuable troubleshooting information
- Three built-in 10/100 Ethernet ports (LAN, WAN, DMZ) for the RF600VPN and the RF660VPN.
    - Three built-in 10/100/1000 Ethernet ports (LAN, WAN, DMZ) for the RF760VPN
- Shared broadband or dedicated Internet access for LAN users with one IP address
- Internet access Control Tools provide client and site filtering and traffic monitoring and reporting
- IP address mapping/port forwarding and DMZ port
- Two-year warranty

Feature Highlights

RouteFinder Applications. The RouteFinder combines Virtual Private Networking (VPN), firewall, e-mail anti-virus protection, and content filtering in one box. It is a cost-effective, easy to manage solution that is ideal for the small to medium business looking to add one or all of the following applications to their network:

Remote User VPN. The client-to-LAN VPN application replaces traditional dial-in remote access by allowing a remote user to connect to the corporate LAN through a secure tunnel over the Internet. The advantage is that a remote user can make a local call to an Internet Service Provider, without sacrificing the company's security, as opposed to a long distance call to the corporate remote access server.

Branch Office VPN. The LAN-to-LAN VPN application sends network traffic over the branch office Internet connection instead of relying on dedicated leased line connections. This can save thousands of dollars in line costs and reduce overall hardware and management expenses.

Firewall Security. As businesses move toward always-on broadband Internet connections, the network becomes more vulnerable to Internet hackers. The RouteFinder provides a full-featured Stateful Packet Inspection firewall to provide security from intruders attempting to access the office LAN.

Email Anti-Virus Protection. An optional email virus protection subscription ensures the network is protected against the latest virus outbreaks.

Content Filtering. A free, one-year URL content filtering subscription allows you to automatically manage what Web content is available.

Plug-and-Play Security Appliance. The RouteFinder plugs in at the Internet connection of each office. It provides three independent network interfaces (LAN, WAN and DMZ) that separate the protected office network from the Internet while offering an optional public network for hosting Web, e-mail, or ftp servers. Each network interface is independently monitored and visually displayed on the front of the RouteFinder.

Secure VPN Connections. The RouteFinder uses IPSec and PPTP industry standard protocols, data encryption, user authentication, and the Internet to provide high-performance, secure VPN connections. For LAN-to-LAN connectivity, the RouteFinder utilizes the IPSec protocol with strong 168-bit 3DES encryption using IKE and PSK key management. In addition, it provides very high performance with 15M bps (RF660VPN) of 3DES encryption throughput. The RF600VPN = 3M bps and the RF760VPN = 50M bps. For client-to-LAN connectivity, Multi-Tech provides optional IPSec client software. The RouteFinder also supports remote users that want to use the PPTP VPN client built into the Windows operating system. This provides 40-bit or 128-bit encryption, user name and password authentication.

State-of-the-Art Firewall Security. The RouteFinder provides network layer security utilizing Stateful Packet Inspection, the sophisticated firewall technology found in large enterprise firewalls, to protect the network against intruders and Denial of Service (DoS) attacks. It also uses Network Address Translation (NAT) to hide internal, non-routable IP addresses and allows internal hosts with unregistered IP addresses to function as Internet-reachable servers. In addition to network layer security, it provides application level security using SMTP, HTTP, DNS, and SOCKS proxies. The RouteFinder also utilizes filters to block specific Internet content to protect against viruses, dangerous ActiveX controls, Java, Javascript, and Cookies. An automatic update feature provides the highest level of security by automatically downloading and installing the latest system software and security patches protecting against any newly discovered hacker attacks with a single click.

Content Filtering. The RouteFinder includes a one-year URL content filtering subscription. It utilizes SurfControl® content categorization list, the world's largest database of Internet content, which includes 5 million Web sites covering over 900 million Web pages. Daily updates of categorized sites are available for download. In addition, it includes URL Access and Deny Reporting. The subscription can easily be renewed on an annual basis.

Automatic Dial Backup. The RouteFinder provides a serial port that, when connected to a dial-up modem or ISDN terminal adapter, can serve as a backup resource for Internet access and VPN tunneling if your cable or DSL service goes down. In addition to the serial port, the RouteFinder RF660VPN and RF760VPN models include a built-in modem.

Optional VPN Client Software. Multi-Tech provides an easy-to-use IPSec VPN client software that transparently secures Internet communications anytime, anywhere. VPN client software is ideal for business users who travel frequently or work from home. It provides secure remote access through the RouteFinder VPN gateway for applications such as remote access, file transfer, e-mail, Web browsing, messaging or IP telephony. Encryption and authentication operations are completely transparent to the end user. In general, IPSec provides stronger encryption than PPTP resulting in better overall security.

Comprehensive Service and Support. The Multi-Tech commitment to service means we provide a two-year product warranty and service that includes telephone technical support, 24-hour web site and FTP support.

E-mail Anti-Virus Protection. Computer viruses are one of the leading security threats to Internet-connected networks. Users can unknowingly download and launch dangerous viruses that can damage data or cause computer crashes. Viruses can also be used as delivery mechanisms for hacking tools, compromising the security of the network, even if a firewall is installed. An optional e-mail virus protection subscription utilizes a high-performance, ICSA-tested, anti-virus engine which checks both incoming and outgoing e-mail for viruses in real-time. Automatic anti-virus updates are downloaded at user-defined intervals to ensure protection is current. The e-mail anti-virus protection can be easily renewed on an annual basis. Ask about our free 30-day evaluation.

User Authentication. To increase the level of security, user identity can be verified before access to Internet services is permitted. The RouteFinder supports authentication at a local user database as well as at external user databases, like Windows 2000 or Radius server.

Robust, Easy-to-Use Management. The RouteFinder includes robust management support allowing a network administrator to securely manage the devices either through a web browser or at the command line. The browser-based option uses the HTTP or HTTPS protocol, also known as SSL (Secure Sockets Layer) to provide 128-bit encryption to secure the management session. The command line interface is accessible via SSH (Secure Shell) and supports SCP (Secure Copy).

Reporting. The RouteFinder also includes a suite of integrated monitoring and reporting tools that help administrators troubleshoot the Internet security system and report to management the usage of the Internet. This includes reporting on system uptime, hardware, and network utilization. HTTP and SMTP proxy reports provide information about any actions needed to handle virus-infected e-mails. The RouteFinder also disables and logs attempted port scans. In addition, it provides accounting reports and a self-monitor that sends an e-mail notification of system-level issues.

Ship Kit Contents

The RouteFinder VPN is shipped with the following:

- One Multi-Tech Systems, Inc. RouteFinder VPN
- One Power Cord
- One printed Quick Start Guide
- One external power supply for the RF600VPN
  Note: The power supply for the RF660VPN and RF760VPN is internal
- Two Rack Mounting Brackets and four mounting screws
- One RouteFinder VPN documentation CD which contains documentation, license agreements, Adobe Acrobat Reader, and License keys
- One RouteFinder VPN Software Recovery CD

Note

If any of these items are missing, contact Multi-Tech Systems or your dealer or distributor. Inspect the contents for signs of any shipping damage. If damage is observed, do not power up the RouteFinder VPN; contact Technical Support at Multi-Tech Systems, Inc. for advice.

Software Recovery CD Warning

Do not use the Software Recovery CD for any purpose except for re-installing software onto the RouteFinder VPN hard drive.

License Keys

System License Key

Each RouteFinder VPN ships with a unique individual system License Key, a 20-digit alphanumeric number. You can enter and view License Key information from the RouteFinder's Web Management software at **Administration > License Key > Open System License Key**. This screen shows the entered License Key number and indicates whether it is a valid License Key number.

The License Key number is tied to and tracked with your RouteFinder's serial number. Whenever you require additional licenses, you must first provide Multi-Tech with your current License Key and serial number information in order for us to update your RouteFinder. With a valid License Key, you are entitled to use Multi-Tech's Update service and support.

What to Do if a Trial License Key Expires

If the license key is a trial key, after expiry of the license period, the WAN interface of the RouteFinder will shut down. If the DHCP client or PPPoE is enabled, they will be disabled. The user can connect to the RouteFinder through the LAN interface and enter another valid license key to proceed further. The user has to manually enable the DHCP client / PPPoE after entering another valid license key.

URL Categorization License Key

An 11-digit numeric key Universal Resource Locator (URL) Categorization License Key is also shipped with your RouteFinder. This Key allows you to set up a URL database that limits clients' access to places on the Internet by blocking sites you do not want accessed. In other words, you can deny users access to various categories of Web sites you select.

AntiVirus License Key

AntiVirus software with its corresponding License Key is available as a special purchase from Multi-Tech.

Where to Find the License Key Number Label

License Key numbers are printed on labels and are located:

- On the bottom of the RouteFinder chassis
- On the hard drive inside the chassis
- On the front cover of the Quick Start Guide.

Additional RouteFinder Documentation

These additional RouteFinder reference documents are included on the system CD and are also posted on the Multi-Tech Web site.

1. The RouteFinder configured with DNAT and aliases.
2. Setting up a PPTP server and a PPTP remote client.
3. The VPN tunnel configured for manual mode example and IPSec pass-through in manual mode example.
4. A quick start guide for the add-on product IPSec SSH client.
5. Hard-Disk Drive Recovery.

Safety Warnings

Lithium Battery Caution

Danger of explosion if battery is incorrectly replaced. A lithium battery on the RouteFinder VPN PC board provides backup power for the time-keeping capability. The battery has an estimated life expectancy of ten years. When it starts to weaken, the date and time may be incorrect. If the battery fails, send the board back to Multi-Tech for battery replacement.

Ethernet Ports Caution

The Ethernet ports are not designed to be connected to a Public Telecommunication Network.

Software Recovery CD Warning

Do not use the Software Recovery CD for any purpose except for re-installing software onto the RouteFinder VPN hard drive.

Telecom Warnings for Modem

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in a wet location unless the jack is specifically designed for wet locations.
- This product is to be used with UL and cUL listed computers.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Avoid using a telephone during an electrical storm. There may be a remote risk of electrical shock from lightening.
- Do not use the telephone to report a gas leak in the vicinity of the leak.
- To reduce the risk of fire, use only No. 26 AWG or larger Telecommunications line cord.

Safety Recommendations for Rack Installations

Ensure proper installation of the ROUTEFINDER in a closed or multi-unit enclosure by following the recommended installation as defined by the enclosure manufacturer. Do not place the ROUTEFINDER directly on top of other equipment or place other equipment directly on top of the ROUTEFINDER.

If installing the ROUTEFINDER in a closed or multi-unit enclosure, ensure adequate airflow within the rack so that the maximum recommended ambient temperature is not exceeded.

Ensure that the ROUTEFINDER is properly connected to earth ground via a grounded power cord. If a power strip is used, ensure that the power strip provides adequate grounding of the attached apparatus.

Ensure that the main supply circuit is capable of handling the load of the ROUTEFINDER. Refer to the power label on the equipment for load requirements.

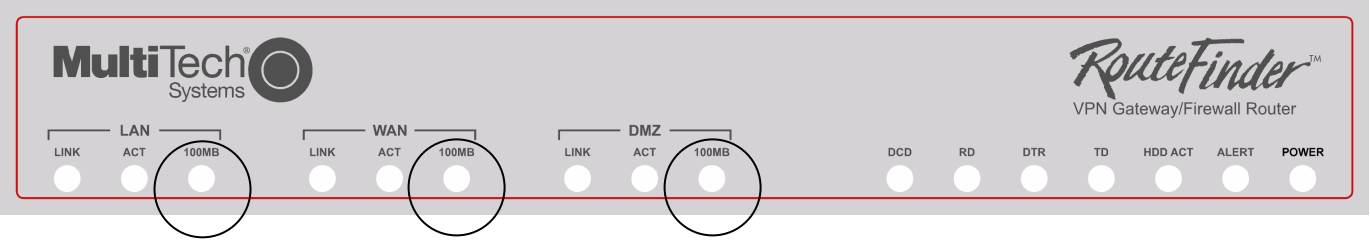
Maximum ambient temperature for the ROUTEFINDER is 50 degrees Celsius (120° F).
This equipment should only be installed by properly qualified service personnel.

Connect like circuits. In other words, connect SELV (Secondary Extra Low Voltage) circuits to SELV circuits and TN (Telecommunications Network) circuits to TN circuits.

RouteFinder Front Panels

RF760/660VPN Front Panel

The R760VPN and the RF660VPN have 16 LEDs that show device and network operating status.



For the RF760VPN, these LEDs are labeled 10/100/1G.

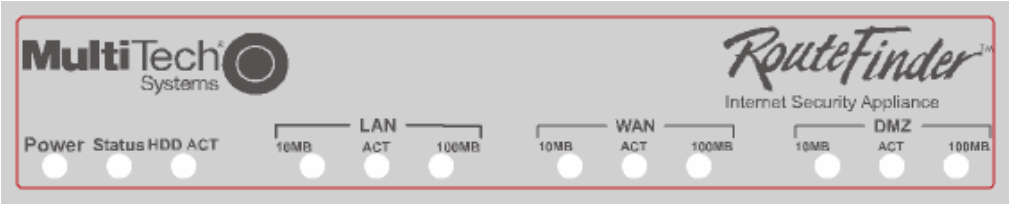
- When 10, the LED is Off.
- When 100, the LED is Green.
- When 1G, the LED is Orange.

RF760 / 660VPN LED Descriptions

LAN LEDs	Description
LINK	LAN LINK LED - Indicates link integrity for the LAN Ethernet port. If the Ethernet link is valid at 10 Mbps, 100 Mbps, or 1G (RF760VPN) the LINK LED is lit. If the Ethernet link is invalid, the LINK LED is off.
ACT	ACT (Activity) LED - Indicates transmit and receive activity on the LAN Ethernet port. When activity is present on the LAN Ethernet port, the ACT LED is lit. When no activity is present on the LAN Ethernet port, the ACT LED is off.
100MB or 10/100/1G	**For the RF760VPN:** If the Ethernet link is valid at 10 Mbps, the LAN LED is off. If the Ethernet link is valid at 100 Mbps, the LED is green. If the Ethernet link is valid at 1G, the LED is orange. **For the RF660VPN:** The LAN 100MB LED is lit if the LAN Ethernet port is linked at 100 Mbps. The LAN 100 MB LED is off at 10 Mbps.
WAN LEDs	**Description**
LINK	WAN LINK LED - Indicates link integrity for the WAN Ethernet port. If the link is valid in either 10 Mbps, 100 Mbps, or 1G (760VPN), the LINK LED is on; if the WAN Ethernet link is invalid, the LINK LED is off.
ACT	WAN ACT (Activity) LED - Indicates either transmit or receive activity on the WAN Ethernet port. When activity is present, the ACT LED is on; when no activity is present, the ACT LED is off.
100MB or 10/100/1G	**For the RF760VPN:** If the Ethernet link is valid at 10 Mbps, the LED is off. If the Ethernet link is valid at 100 Mbps, the LED is green. If the Ethernet link is valid at 1G, the LED is orange. **For the RF660VPN:** The 100MB LED is lit if the LAN Ethernet port is linked at 100 Mbps. The 100 MB LED is off at 10 Mbps.
DMZ LEDs	**Description**
LINK	DMZ LINK LED - Indicates link integrity for the DMZ Ethernet port. If the link is valid in either 10 Mbps, 100 Mbps, or 1G (760VPN) the LINK LED is on; if the DMZ Ethernet link is invalid, the LINK LED is off.
ACT	ACT (Activity) LED - Indicates either transmit or receive activity on the DMZ Ethernet port. When activity is present, the ACT LED is lit. When no DMZ Ethernet port activity is present, the ACT LED is off.
100MB or 10/100/1G	**For the RF760VPN:** If the Ethernet link is valid at 10 Mbps, the LED is off. If the Ethernet link is valid at 100 Mbps, the LED is green. If the Ethernet link is valid at 1G, the LED is orange. **For the RF660VPN:** The 100MB LED is lit if the LAN Ethernet port is linked at 100 Mbps. The 100 MB LED is off at 10 Mbps.
Modem	**Description of Modem LEDs**
DCD	DCD (Data Carrier Detect) LED - Lights when the modem detects a valid carrier signal from another modem; on when the modem is communicating with the other modem and off when the link is broken.
RD	RD (Read Data) LED - Flashes when the modem is receiving data from another modem.
DTR	DTR (Data Terminal Ready) LED - Lights when the operating system detects and initializes the modem.
TD	TD (Transmit Data) LED - Flashes when the modem is transmitting data to another modem.
System	**Description of System LEDs**
HDD ACT	HDD ACT (Hard Disk Drive Activity) LED - Lights when the hard disk drive is accessed.
ALERT	ALERT LED - Not used.
POWER	POWER LED - Off when the RouteFinder is in a reset state. When lit, the RouteFinder is not in a reset state.

RF600VPN

The RF600VPN has 12 front panel LEDs that show the network operating status.

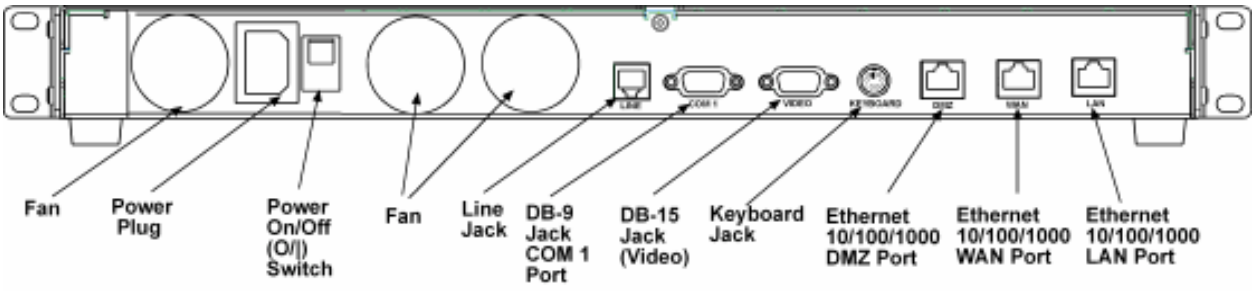


General LED Descriptions	
POWER	POWER LED - Off when the RF600VPN is in a reset state. When the POWER LED is lit, the RF600VPN is not in a reset state.
STATUS	STATUS LED - Off when the RF600VPN is booting up.
HDD ACT	HDD ACT (Hard Disk Drive Activity) LED - Lights when the RF600VPN hard disk drive is accessed.
LAN, WAN, DMZ LED Descriptions	
10MB	10MB LED - Lights when the LAN client has a valid link at 10MB.
ACT	ACT (Activity) LED - Indicates either transmit or receive activity on the LAN Ethernet port. When activity is present on the LAN Ethernet port, the ACT LED is lit. When no activity is present on the LAN Ethernet port, the ACT LED is off.
100MB	100MB LED - Lights when the LAN client has a valid link at 100MB.

RouteFinder Back Panels

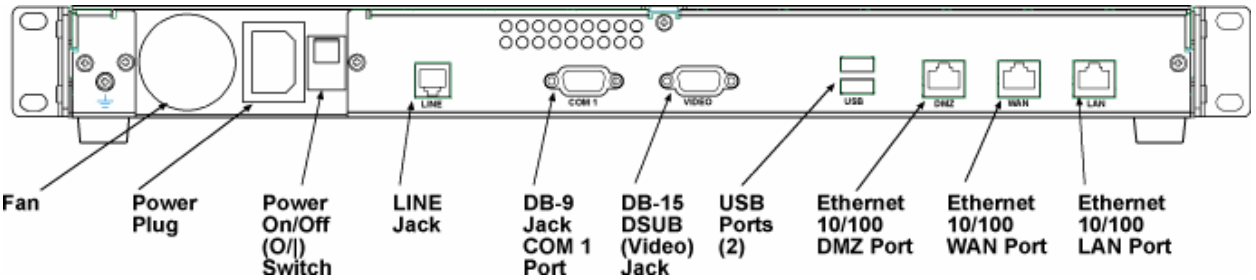
RF760VPN Back Panel

The RF760VPN back panel has three fans, a power plug, a **POWER** Switch (**| / O**), an RJ-11 **LINE** jack, a DB-9 **COM1** jack, a DB-15 High-density DSUB (**VIDEO**) jack, a keyboard jack, an Ethernet 10/100/1000 DMZ Port, and an Ethernet 10/100/1000 WAN Port, and an Ethernet 10/100/1000 LAN Port.



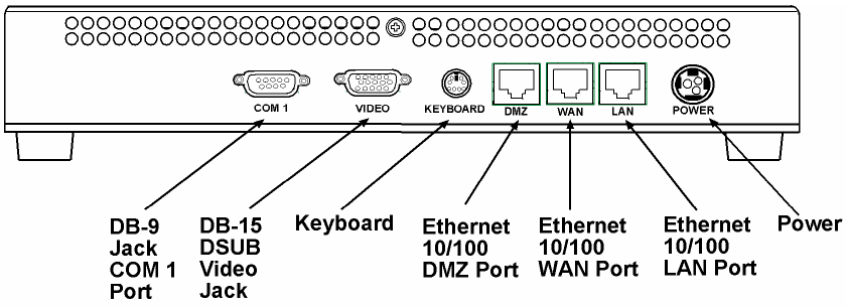
RF660VPN Back Panel

The RF660VPN back panel has a fan, a power plug, the **POWER** Switch (**| / O**), an RJ-11 **LINE** jack, a DB-9 **COM1** jack, a DB-15 High-density DSUB (**VIDEO**) jack, two **USB** (Revision 1.1 compliant) jacks, an RJ-45 **DMZ** jack, an RJ-45 (**WAN**) jack, and an RJ-45 (**LAN**) jack.



RF600VPN Back Panel

The RF600VPN back panel has a DB-9 **COM1** jack, a DB-15 High-density DSUB (**VIDEO**) jack, a keyboard jack, an RJ-45 **DMZ** jack, an RJ-45 **WAN** jack, an RJ-45 **LAN** jack, and a **POWER** jack.



Specifications

Appliance Features	RF760VPN	RF660VPN	RF600VPN
Ethernet Ports	3x10/100/1000BaseT (LAN,WAN, DMZ)	3x10/100BaseT (LAN,WAN, DMZ)	3x10/100BaseT (LAN,WAN, DMZ)
Number of Network Users	Unlimited	Unlimited	Unlimited
Rackmount or Standalone	Both	Both	Both
VPN Features	**RF760VPN**	**RF660VPN**	**RF600VPN**
Remote User (Client-to-LAN)	Yes	Yes	Yes
Branch Office (LAN-to-LAN)	Yes	Yes	Yes
3DES Encryption	Yes	Yes	Yes
3DES Throughput	50M bps	15M bps	3M bps
Protocols	**Security:** IPSec, IKE, NAT, PPTP, HTTPS, SSH, SCP **Authentication:** Shared secret and built-in authentication server **Network:** TCP/IP, DNS **Filtering:** Protocol, port number, and IP address **Proxies:** HTTP, SMTP, DNS, SOCKS	**Security:** IPSec, IKE, NAT, PPTP, HTTPS, SSH, SCP **Authentication:** Shared secret and built-in authentication server **Network:** TCP/IP, DNS **Filtering:** Protocol, port number, and IP address **Proxies:** HTTP, SMTP, DNS, SOCKS	**Security:** IPSec, IKE, NAT, PPTP, HTTPS, SSH, SCP **Authentication:** Shared secret and built-in authentication server **Network:** TCP/IP, DNS **Filtering:** Protocol, port number, and IP address **Proxies:** HTTP, SMTP, DNS, SOCKS
Recommended Number of Tunnels (IPSec)	100	50	25
Recommended Number of Tunnels (PPTP)	100	50	25
Firewall Features	**RF760VPN**	**RF660VPN**	**RF600VPN**
Throughput	300M bps	80M bps	20M bps
Anti-Virus Option	Yes	Yes	Yes
Content Filtering	Yes	Yes	Yes
Application Proxies	Yes	Yes	Yes
Port and IP Filtering	Yes	Yes	Yes
Denial of Service Protection (DoS)	Yes	Yes	Yes
Stateful Packet Inspection	Yes	Yes	Yes
Network Address Translation (NAT)	Yes	Yes	Yes
Virtual Server	Yes	Yes	Yes
Port Scan	Yes	Yes	Yes
Intrusion Detection/Notification	Yes	Yes	Yes
H.323 Pass Through	Yes	Yes	Yes
Management Features	**RF760VPN**	**RF660VPN**	**RF600VPN**
Email Alert	Yes	Yes	Yes
Local & Remote Management	Yes	Yes	Yes
Logging	Yes	Yes	Yes
Reporting	Yes	Yes	Yes
Web Based (HTTP, HTTPS/SSL)	Yes	Yes	Yes
Secure Shell (SSH)	Yes	Yes	Yes
Syslog	Yes	Yes	Yes
Other Features	**RF760VPN**	**RF660VPN**	**RF600VPN**
Shared Internet Access	Yes	Yes	Yes
Automatic Dial-Backup	Yes	Yes	Yes
Integrated Modem	Yes	Yes	No
PPPoE	Yes	Yes	Yes
DHCP Client/Server	Yes	Yes	Yes
User Authentication	Yes	Yes	Yes
Automatic Firmware Downloads	Yes	Yes	Yes
Warranty	2 Years	2 Years	2 Years

Power & Physical Description	RF760VPN	RF660VPN	RF600VPN
Power - Voltage & Frequency	100-240v AC, 50-60 Hz	100-240v AC, 50-60 Hz	100-240v AC, 50-60 Hz
Power Consumption	50 Watts	30 Watts	15 Watts
Physical Description	**Dimensions:** 17" w × 1.75" h × 10.5" d; (43.18cm × 4.45cm × 26.67cm) **Weight:** 10 lbs. (4.54 kg)	**Dimensions:** 17" w × 1.75" h × 10.5" d; (43.18cm × 4.45cm × 26.67cm) **Weight:** 10 lbs. (4.54 kg)	**Dimensions:** 12" w × 1.7" h × 8" d; (30.4cm × 4.4cm × 20.3cm) **Weight:** 5.8 lbs. (2.6 kg)
Operating Environment	**Temperature Range:** 32° to 120° F (0-50°C) **Humidity:** 25-85% noncondensing	**Temperature Range:** 32° to 120° F (0-50°C) **Humidity:** 25-85% noncondensing	**Temperature Range:** 32° to 120° F (0-50°C) **Humidity:** 25-85% noncondensing
Approvals	FCC Part 68 FCC Part 15 (Class A) CE Mark UL60950 ICSA Firewall Certified	FCC Part 68 FCC Part 15 (Class A) CE Mark UL60950 ICSA Firewall Certified	FCC Part 68 FCC Part 15 (Class A) CE Mark UL60950 ICSA Firewall Certified

Overview of RouteFinder VPN Technology

Before we look at how the RouteFinder works and how to use it, we will illustrate why the RouteFinder is necessary for the protection of networks, as well as show which problems and risks exist without an appropriate security system.

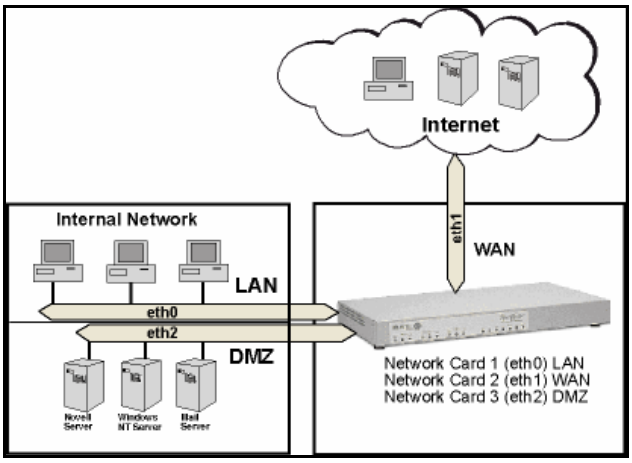
Networks

The systems in the global network communicate via the Internet Protocol Family (IP), including TCP, UDP, or ICMP. The IP addresses are the basis of this communication. They identify all available units within the network.

The Internet itself is actually just a collection of computer networks around the world of varying shape, size, and speed. Where two or more networks join, a whole host of tasks arise, which are dealt with by routers, bridges, or gateways. A special type of connection between two networks is called a firewall.

Generally speaking, three types of networks meet at the firewall:

1. External network/Wide Area Network (WAN)
2. Internal Network/Local Area Network (LAN)
3. De-Militarized Zone (DMZ)



The Firewall

The characteristic tasks of a firewall as a connection between WAN, LAN and DMZ are:

- Protection from unauthorized access
- Access control
- Ensure information integrity
- Perform analysis of protocols
- Alert the administrator of relevant network events
- Conceal internal network structure
- Decoupling of servers and clients via proxies
- Ensure confidentiality

There are several generic network components that, brought together under the heading Firewall, are responsible for these tasks. The following sections provide a brief look at some of the forms and their derivatives.

Network Components That Work with the Firewall

Network Layer Firewalls: Packet Filter

As the name suggests, the Packet Filter is where IP packets (consisting of address information, some flags, and the payload) are filtered. With this kind of firewall you can grant or deny access to services, according to different variables. Some of these variables are:

- The source address
- The target address
- The protocol (e.g. TCP, UDP, ICMP)
- The port number

The great advantage of a network layer firewall is its independence of both the operating system and the applications running on the machine.

In more complex network layer firewall implementations, the packet filtering process includes the interpretation of the packet payload. The status of every current connection is analyzed and recorded. This process is called stateful inspection.

The packet filter records the state of every connection and lets only those packets pass that meet the current connection criteria. This is especially useful for establishing connections from a protected network to an unprotected network.

If a system establishes a connection to a protected network, the Stateful Inspection Packet Filter lets a host's answer packet pass back into the protected network. If the original connection is closed, no system from the unprotected network can send packets into the protected network any longer – unless you explicitly allow it.

Well Known Ports are controlled and assigned by the IANA, and on most systems, can only be used by system (or root) processes or by programs run by privileged users. Ports are used in TCP (RFC793) to name the ends of logical connections which carry long term conversations; and, typically, these same port assignments are used with UDP (RFC768). The assigned ports are in the range 0-1023. IETF RFC 1700 provides a list of the well-known port number assignments. IETF RFCs are available on the Internet from a number of sources.

Application Layer Gateways: Proxies

A second significant type of firewall is the application layer gateway. It is responsible for buffering connections between exterior systems and your system. Here, the packets aren't directly passed on, but a sort of translation takes place, with the gateway acting as an intermediary stop and translator.

The application gateway buffering processes are called proxy servers, or, for short, proxies. Every proxy can offer further security features for its designed task. Proxies generally offer a wide range of security and protocol options.

Each proxy serves only one or a few application protocols, allowing high-level security and extensive logging and analysis of the protocol's usage.

Examples of existing proxies are:

- The SMTP proxy - Responsible for email distribution and virus checking.
- The HTTP proxy - Supporting Java, JavaScript, ActiveX-Filter, and ad banner filtering.
- The SOCKS proxy (the generic circuit-level proxy) - Supporting applications such as FTP clients, ICQ, IRC, or streaming media.

Application level gateways offer the advantage of physical and logical separation of the protected and unprotected networks. They make sure that no packet is allowed to flow directly between networks, resulting in higher security.

Protection Mechanisms

Further mechanisms ensure added security. Specifically, the use of private IP addresses in combination with Network Address Translation (NAT) in the form of:

- Masquerading
- Source NAT (SNAT)
- Destination NAT (DNAT)

These allow a whole network to hide behind one or a few IP addresses, preventing the identification of your network topology from the outside.

With these protection mechanisms in place, Internet connectivity remains available, but it is no longer possible to identify individual machines from the outside.

By using Destination NAT (DNAT), it is still possible to place servers within the protected network/DMZ and make them available for an assigned service.

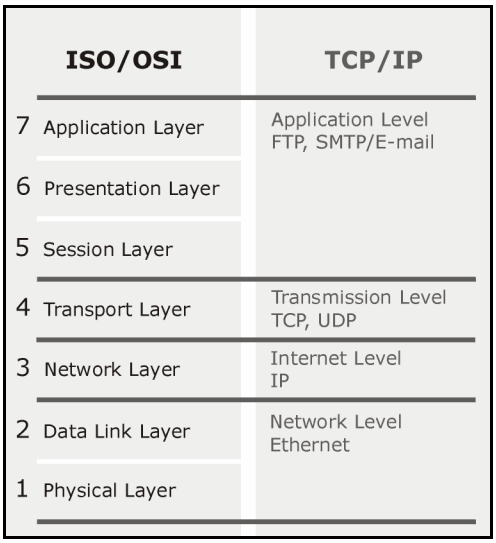
In the sample graphic above, a user with the IP 5.4.3.2, port 1111 sends a request to the Web server in the DMZ. Of course, the user knows only the external IP (1.1.1.1, port 80). Using DNAT, the RouteFinder now changes the external IP address to 10.10.10.99, port 80 and sends the request to the Web server. The Web server then sends the answer with its IP address (10.10.10.99, port 80) and the user's IP. The RouteFinder recognizes the packet by the user address, and it then changes the internal IP (10.10.10.99, port 80) into the external IP address (1.1.1.1, port 80).

To satisfy today's business world needs, the IT infrastructure must offer real-time communication and co-operate closely with business partners, consultants, and branches. Increasingly, the demand for real-time capability is leading to the creation of extranets that operate either:

- via dedicated lines, or
- unencrypted lines via the Internet

Each of these methods has advantages and disadvantages, as there is a conflict between the resulting costs and the security requirements.

Virtual Private Networking (VPN) establishes secure (i.e., encrypted) connections via the Internet, an important function especially if your organization operates at several locations that have Internet connections. These secure connections use the IPSec standard derived from the IP protocol IPv6.



ISO Layers and TCP/IP

Once set up, this encrypted connection is used automatically (i.e., without extra configurations or passwords at the client systems) regardless of the type of data that is to be transferred. This protects the content during the transport. At the other end of the connection, the transferred data is transparently decoded and is available for the recipient in its original form.

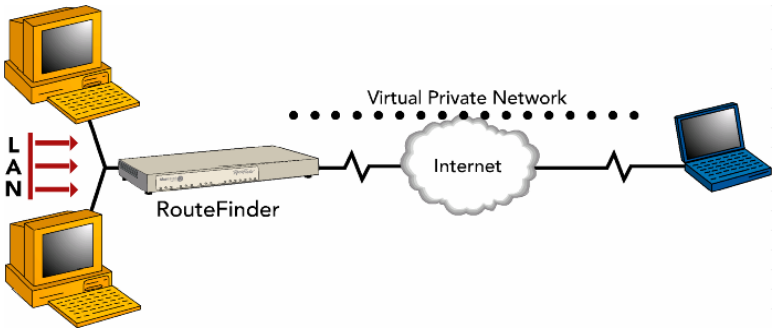
The RouteFinder VPN uses a hybrid of the above listed basic forms of firewalls and combines the advantages of both variations: the stateful inspection packet. Stateful inspection packet filter functionality offers platform-independent flexibility, and the ability to define, enable or disable all necessary services. Existing proxies make the RouteFinder an application gateway that secures vital client system services, such as HTTP, Mail, and DNS by using a proxy. The ROUTEFINDER also enables generic circuit-level proxy via SOCKS.

VPN, Source NAT, Destination NAT, masquerading, and the ability to define static routes make the dedicated firewall an efficient distribution and checkpoint in your network.

Typical Applications

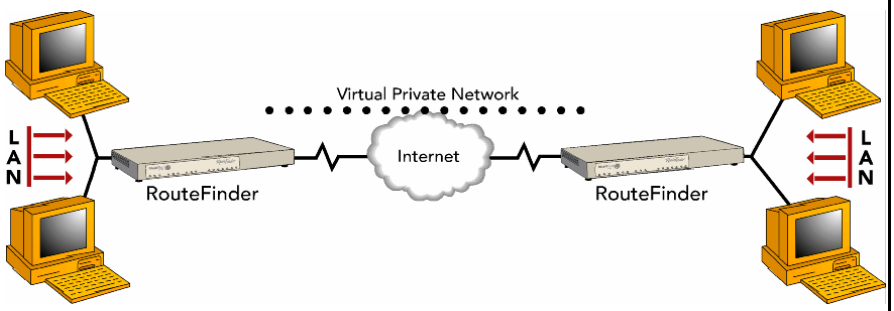
Remote User VPN

The client-to-LAN VPN application replaces traditional dial-in remote access by allowing a remote user to connect to the corporate LAN through a secure tunnel over the Internet. The advantage is that a remote user can make a local call to an Internet Service Provider, without sacrificing the company's security, as opposed to a long distance call to the corporate remote access server.



Branch Office VPN

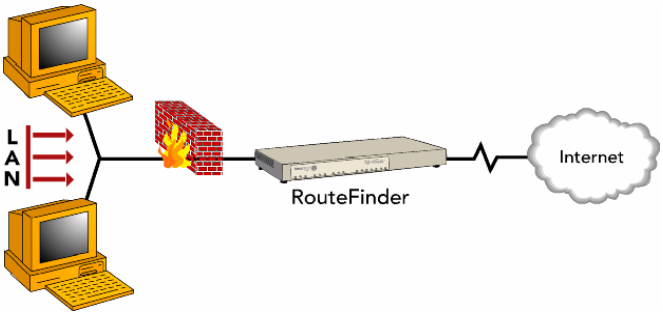
The LAN-to-LAN VPN application sends network traffic over the branch office Internet connection instead of relying on dedicated leased line connections. This can save thousands of dollars in line costs and reduce overall hardware and management expenses.



Firewall Security

As businesses shift from dial-up or leased line connections to always-on broadband Internet connections, the network becomes more vulnerable to Internet hackers.

The RouteFinder VPN provides a full-featured firewall based on Stateful Packet Inspection technology and NAT protocol to provide security from intruders attempting to access the office LAN.



Chapter 2 – Installation

Pre-Installation Planning

Planning and Establishing the Corporate Security Policy

Having an organization-wide security policy is the first, and perhaps most, important step in general security planning. Organizations without a well-devised top-level security policy will not have ready answers to questions such as:

- Who is allowed access to which servers?
- Where are the backups stored?
- What is the recovery procedure for a security breach?

These questions must be answered in terms of security costs, usability, compatibility with internal "culture", and alignment with your site's legal requirements.

Putting a security policy in place and keeping abreast of new security issues as they arise are paramount to securing your network.

Contents of a Corporate Internet Security Policy

The policy statements should be clear, easy to understand, and supported by management.
All enterprises should have a carefully planned security policy that protects their network. Your security policy should define both what should be protected as well as how it should be protected. A comprehensive, clear, and well-communicated security policy is an important first step in protecting any network from the many threats associated with the power of the Internet.

A corporate Internet security policy should cover at least 6 major areas, including:

1. **Acceptable Use** – Define the appropriate use of the network and other computing resources by any and all users. This should include policy statements like: “password sharing is not permitted"; "users may not share accounts"; and "users may not make copies of copyrighted software.”
2. **Remote Access** – Outline acceptable (and unacceptable) means of remotely connecting to the internal network. Cover all of the possible ways that users remotely access the internal network, such as dial-in, ISDN, DSL, cable modem, Telnet, and others. Specify who is allowed to have remote access as well as how users may obtain remote access. The security policy must also address who is allowed high-speed remote access and any extra requirements associated with that privilege (e.g., all remote access via DSL requires that a firewall be installed). You will also want to define users' email security here (e.g., in MS Outlook at **Tools > Options > Security > Zone Settings > Security Settings**).
3. **Information Protection** – Provide guidelines to users that define the use and transmission of sensitive information to ensure the protection of your enterprise’s key elements of information (e.g., set a standard for encryption level (such as 3DES) for information sent over the Internet).
4. **Firewall Management** – Define how firewall hardware and software are managed. This includes change requests and approval, periodic review of firewall configurations, and firewall access privilege settings.
5. **Special Access** – Provide guidelines for any special, non-standard needs for access to specialized networks or systems.
6. **Network Connection** – Establish policies for adding new devices and new users to the network, with an approval process, along with the associated security requirements.

Planning the Network

Before installing, you should plan your network and decide which computer is to have access to which services. This simplifies configuration and saves you a lot of time that you would otherwise need for corrections and adjustments.

Establishing an Address Table

Enter the configuration information (e.g., the IP addresses used, Net Mask addresses, and the Default Gateway) into the appropriate field of the Address Table below. Please print this page and use it to fill in your specific ROUTEFINDER and network information (e.g., the IP address used, email lists, etc.), and keep it for future reference.

	IP Address	Net Mask	Default Gateway
Network Card connected to the internal network (LAN on eth0)	___.___.___.___	___.___.___.___	
Network Card connected to the external network (WAN on eth1)	___.___.___.___	___.___.___.___	___.___.___.___
Network Card connected to the DMZ (eth2)	___.___.___.___	___.___.___.___	

System Administrator Required Planning

The system administrator must complete these setup requirements before installing the ROUTEFINDER software:

- Set the correct configuration of the Default Gateway
- Install an HTTPS-capable browser (e.g., the latest version of Microsoft Internet Explorer or Netscape Navigator)
- Activate JavaScript and Cascading Style Sheets
- Make sure that no proxies are entered in the browser
- If Secure Shell (SSH) is to be used, you must install an SSH client program (e.g., **PuTTY** in Windows 2000 or the bundled SSH client in most Linux packages).

Installation Overview

RouteFinder VPN installation is divided into four steps:

1. Hardware installation
2. Cabling
3. Software initial configuration
4. RouteFinder configuration

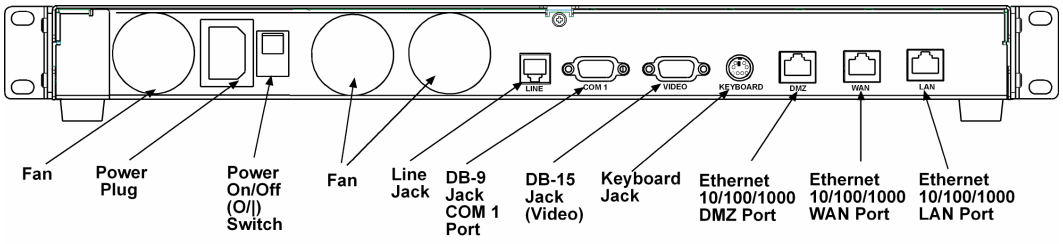
Hardware Installation Procedure

The RouteFinder VPN is designed to install either on a desktop or in a standard EIA 19" rack and is shipped with the mounting hardware to install the RouteFinder VPN in the standard EIA 19" rack. If installing in a rack, use the provided mounting hardware and follow the rack enclosure manufacturer's instructions to safely and securely mount the RouteFinder the rack enclosure. Proceed to the cabling procedure.

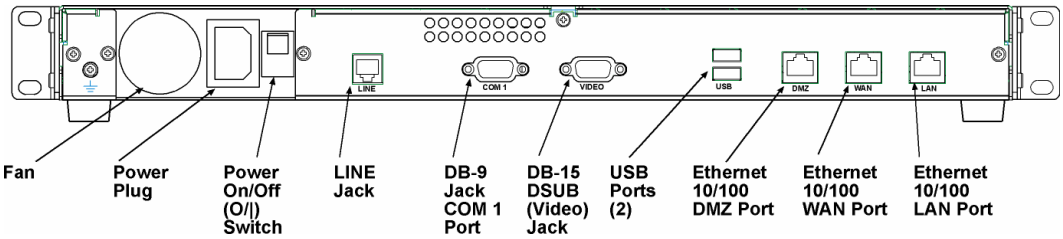
Cabling Overview

Cabling your RouteFinder VPN involves making the proper Power, DMZ, WAN and LAN connections as illustrated and described below.

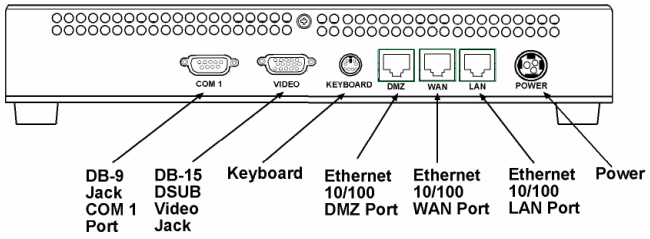
RF760VPN



RF660VPN



RF600VPN



1. Using an RJ-45 Ethernet cable, connect the DMZ RJ-45 jack to the DMZ device or network (Optional – for example, a Voice over IP gateway).
2. Using an RJ-45 Ethernet cable, connect the WAN RJ-45 jack to the device for the external network.
3. Using an RJ-45 Ethernet cable, connect the LAN RJ-45 jack to the internal network switch or hub.
   Note: Use a cross-over Ethernet cable if connecting to a single device.
4. With the RF760 or RF660 RouteFinder VPN Power switch in the off (O) position and using the supplied power cord, plug one end into the RouteFinder VPN connect power plug and the other end into a live power outlet.
   Note: The status LED blinks continuously after power-up.
5. Wait for the RouteFinder VPN to beep five times, indicating that it is ready to be configured with a Web browser.

Shutdown Caution: Never switch off the RouteFinder VPN Power until after you have performed the **Shutdown** process. If the RouteFinder VPN is not properly shut down before switching off Power, the next startup may take a little longer, or in the worst case, data could be lost.

Setting up a Workstation and Starting the RouteFinder VPN

This section of the Quick Start Guide covers the steps for setting up a workstation that is connected to the RouteFinder VPN, starting up the RouteFinder VPN, opening the RouteFinder VPN Web Management program, performing the time zone setup, and using the Menu bar to navigate through the Web Management software screens.

Connections

1. Connect a workstation to the RouteFinder's **LAN** port via Ethernet. Connections are described on the previous page.

   Note: If not using a hub, use a cross-over cable to connect a PC NIC to the RouteFinder's Ethernet 10/100 LAN Port.
2. Set the workstation IP address to **192.168.2.x** subnet.
3. Obtain an Internet Public IP address so it can be assigned to the WAN port.
4. Connect to the Internet at the RouteFinder **WAN** port.

Power Up

5. Turn on power to the RouteFinder VPN. After several minutes, you will hear 5 beeps signifying the software has fully booted.

   Note: If you hear a continuous beep or no beep, cycle RouteFinder VPN power, connect an external monitor and check the hard drive.

Open a Web Browser

6. Bring up a Web browser on the workstation. Type the default Gateway address: **https://192.168.2.1** and press the **Enter** key.

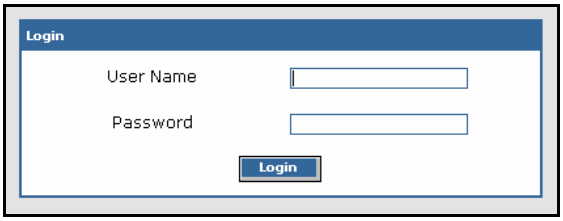
   IMPORTANT: Be sure to type **https** (**http** will not work).

   Note: Make sure your PC's IP address is in the same network as the router's IP address. **WINIPCFG** and **IPCONFIG** are tools for finding a computer's default gateway and MAC addresses. In Windows 98/ME you can type **WINIPCFG**. In Windows 2000/NT/ME/XP, you can type **IPCONFIG**.

7. In some environments, one or more Security Alert screen(s) may display. At the initial Security Alert screen, click Yes and follow any additional on-screen prompts.

Login

8. The Login screen is displayed.



- Type the default User name: **admin** (all lower-case).
- Tab to the Password field and type the default password: **admin** (all lower-case).
- Click the **Login** button.

Note: The **User name** and **Password** entries are case-sensitive (both must be typed in lower-case). The password can be up to 12 characters. Later, you will want to change the password from the default (**admin**) to something else. If Windows displays the **AutoComplete** screen, you may want to click **No** to tell Windows OS to not remember the password for security reasons.

Password Caution: Use a safe password! Your first name spelled backwards is not a sufficiently safe password; a password such as xfT35$4 is better.

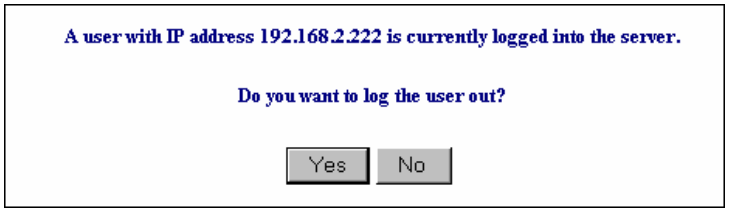
It is recommended that you change the default password. Do not keep this default password; create your own password.

9. If someone else is already logged onto the RouteFinder VPN or you were logged in recently, the following message displays.

Do you want to log the user out?

Click **Yes**.

If you click **No**, you are returned to the Login screen.

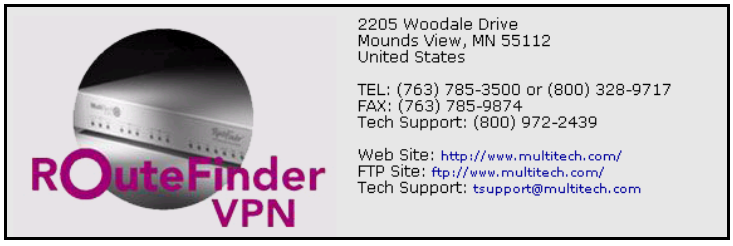


Web Management Software Opens

The Web Management **Home** screen is displayed. Web Management software is factory-installed on your RouteFinder.

(This is a view of the top part of the Home screen.)

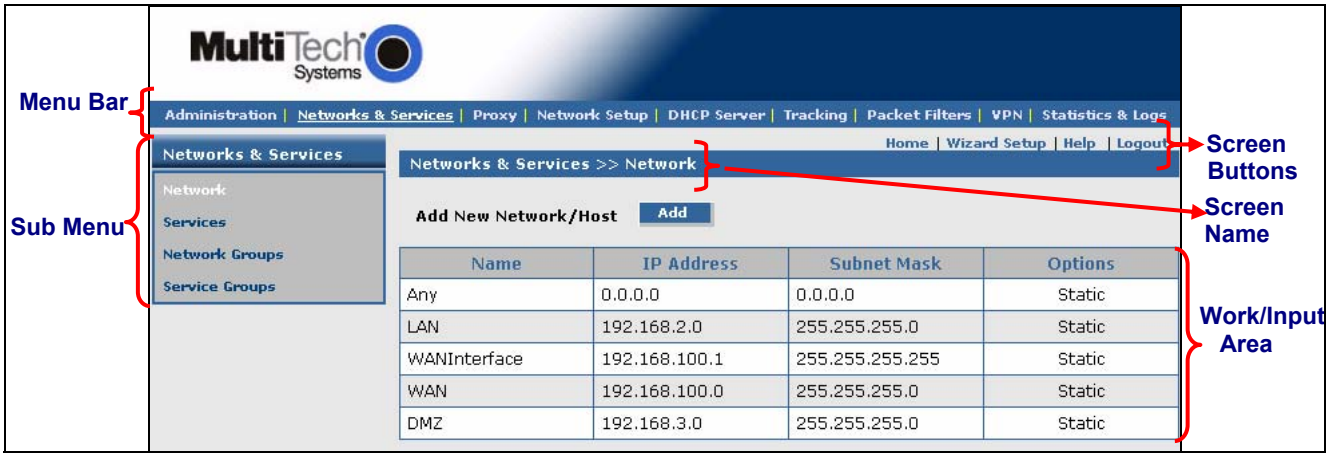
(This is a view of the Multi-Tech Systems, Inc. informational part of the Home screen.)



Navigating Through the Screens

Before using the software, you may find the following information about navigating the screens and the structuring of the menus helpful.

The Web Management Screen



RouteFinder Menu Bar

Menu Selections

Administration	Set up system parameters, Administrative Access, User Authentication; enter licenses and certificates, etc. See entire list of functions on next page.
Networks & Services	Define networks, services, and groups to make them available to be used by other functions such as allowed networks, packet filters, VPN, and proxies.
Proxy	Set up proxies.
Network Setup	Set up the LAN, WAN, and DMZ Ethernet ports; PPP modem link, etc.
DHCP Server	Configure the DHCP server settings.
Tracking	Set up tracking of all packets through the network ports in the RouteFinder VPN, set up automatic download and upgrade of packages from a specified Update server, set up import/export backup configurations.
Packet Filters	Define filter rules and ICMP rules.
VPN	Virtual Private Network. Set up a secure communication tunnel to specific Internet systems.
Statistics & Logs	View and download all the statistics and log files maintained by your system.

Screen Buttons

Home	The main screen.
Wizard Setup	Change passwords and quickly set up your RouteFinder VPN with the basic configuration that will set it up as a firewall.
Help	Describes what to do on each screen.
Logout	Logout and return to the login screen.

Sub-Menu

Each item on the Menu Bar has its own sub-menu which displays on the left side of the screen.

When you click one of the Menu Bar buttons, the screen that displays is the first sub-menu option. You can choose other sub-menu screens by clicking the screen name in the sub-menu.

This is an example of the **Administration** sub-menu. It displays when **Administration** is clicked on the Menu Bar.

Menus and Sub-Menus

Administration	Networks & Services	Proxy	Network Setup	DHCP Server
System Setup	Network	HTTP Proxy	Interface	Subnet Settings
SSH	Services	Custom Filters	PPP	Fixed Addresses
SNTP Client	Network Groups	SMTP Proxy	PPPoE	
Administrative Access	Service Groups	SMTP SPAM Filtering	DHCP Client	
Site Certificate		POP3 Proxy	Dynamic DNS	
License Key		POP3 SPAM Filtering	Routes	
Intrusion Detection		SOCKS Proxy	Masquerading	
Tools		DNS Proxy	SNAT	
System Scheduler			DNAT	
Factory Defaults				
User Authentication				
Local Users				
Radius & SAM				
Restart				
Shutdown				

Tracking	Packet Filters	VPN	Statistics & Logs
Accounting	Packet Filter Rules	IPSec	Uptime
Update Services	ICMP	X.509 Certificates	Hardware
Backup	Advanced	IPSec Bridging	Networks
Version Control	Enable/Disable Log	PPTP	Interfaces
			SMTP Proxy
			Accounting
			Self Monitor
			IPSec
			PPTP
			Packet Filter
			Port Scans
			View Logs
			HTTP Access
			DHCP
			SMTP Virus Quarantine
			POP3 Virus Quarantine
			SMTP SPAM Quarantine
			Administrative Authentication Log

Chapter 3 – Configuration

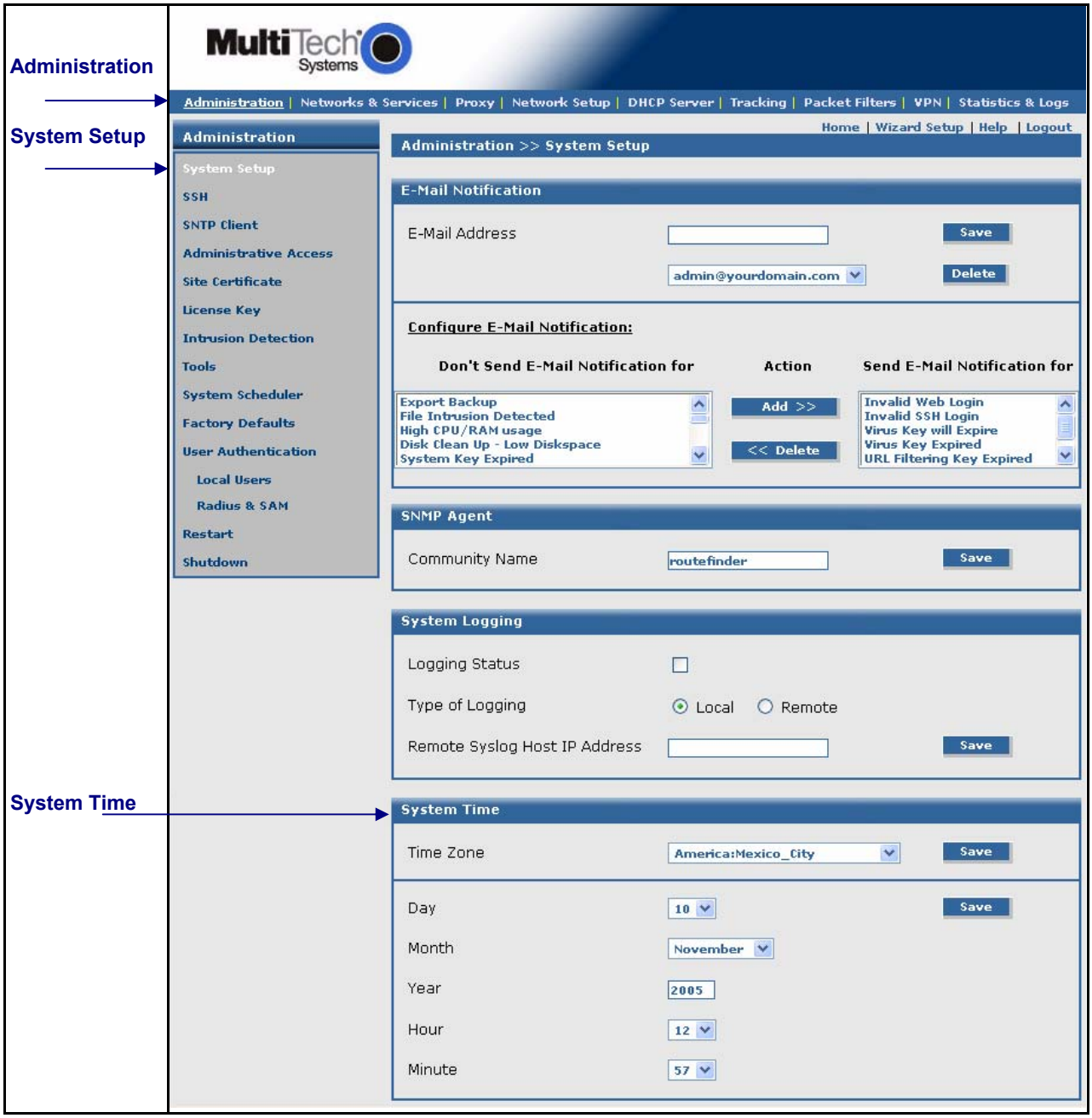
Initial Configuration Step

Set Up Your Time Zone

Click **Administration** on the menu bar. The **System Setup** screen displays.

Set the following:

- Set **System Time** by selecting your **Time Zone**
- Set the current **Day**, **Month**, **Year**, **Hour**, and **Minute**

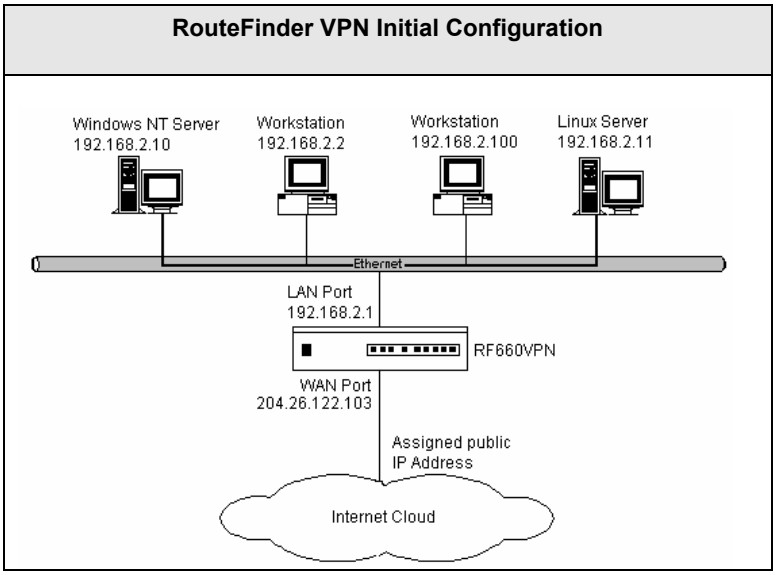


Second Configuration Step

Using the Wizard Setup is a quick way to enter the basic configuration parameters to allow communication between the LAN's workstation(s) and the Internet as shown in the example below.

Important Note: An initial configuration must be completed for each type of RouteFinder functions: firewall configuration, LAN-to-LAN configuration, a LAN-to-Remote Client configuration.

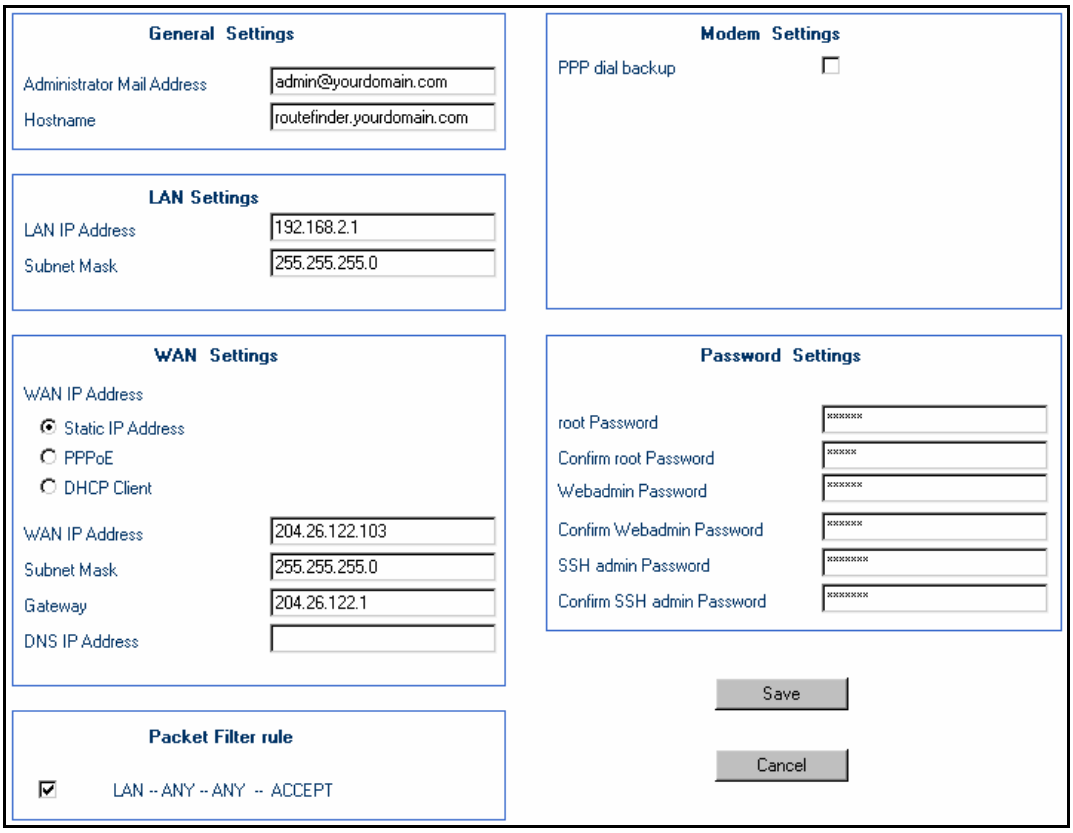
Note About License Agreements: It is suggested that you read the legal information and license agreement before beginning the configuration. This information can be found in the Appendix.



The addresses used in this example are entered through the Wizard Setup. See the screen example on the next page.

The Wizard Setup Screen

Click on the **Wizard Setup** button. The following screen displays.



1. Enter your **Administrator Email Address** (can be anything).
   Example: admin@yourdomain.com
2. Enter your **Hostname** for the RouteFinder (can be anything).
   Example: routefinder.domainname.com
3. **LAN IP Address** and **Subnet Mask** default into the fields. This should be acceptable for your site.
4. Enter the **WAN IP Address.** This is the PUBLIC STATIC IP address.
   Set this option based on information provided by your ISP. Example: 204.26.122.103
5. Change the **Gateway IP address**; this is the IP address of the router that connects to the Internet.
   Example: 204.26.122.1
6. Place a checkmark in the **Packet Filter Rule LAN-ANY-ANY-ALLOW** box. This will enable the rule.
7. Change **Password Settings** as appropriate for your network. It is highly recommended that you change all default passwords. Do not leave them at the defaults.
8. Click **Save** to save the settings you just entered.
9. The following message displays. Click **OK** to close the message box and save your changes.

   Click OK to save the changes. Please be patient. Wizard Setup will take a few minutes to implement the changes. Do not close the Browser.

10. One more message displays. Note that saving your settings will take 1-2 minutes.

    Please do not close the browser. Server is saving the values. After a few minutes you will be redirected to the new IP address. If you are not redirected, change the address in the location bar to 192.168.2.1.

11. Test your workstation to see that it can access the Internet. If a connection is established, then the settings have been entered correctly.

Your Basic Configuration Is Now Complete

Chapter 4 – Configuration Examples

Example 1 – LAN-to-LAN VPN (Branch Office)

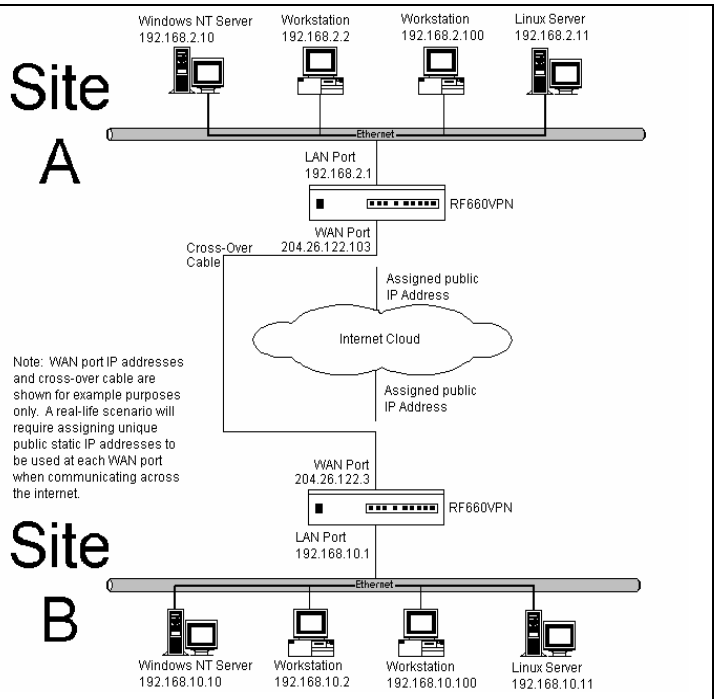
The setup for a LAN-to-LAN VPN (branch office) requires two RF660VPNs - one in the home office and one in the remote branch office. It requires additional parameters beyond the Wizard Setup to be entered; these are listed in the table below.

For the RouteFinder VPN in remote branch office follow the same procedures as the home office procedures; just use different IP addresses. The addresses and parameters in this example are used throughout this section as a point of reference for you.

For details about this and other setups, see the RouteFinder Setup Examples Reference Guide, which is available on the RouteFinder CD and on the Multi-Tech Systems, Inc. Web site at http://www.multitech.com

Site A - Static IP Addresses (Input these parameters using the RF660VPN in the home office).

1. Domain name = site-A.com
2. Public Class C = 204.26.122.x
3. Networks & Services > Networks
   LAN: 192.168.2.0 – 255.255.255.0
   RemoteLAN: 192.168.10.0 – 255.255.255.0
   RemoteWAN_IP: 204.26.122.3 – 255.255.255.255
4. Network Setup > Interface
   Default gateway = 204.26.122.1
   Host name = RF660VPN.site-A.com
   Eth0 = LAN, 192,168.2.1, 255.255.255.0
   Eth1 = WAN, 204.26.122.103, 255.255.255.0
   Eth2 = DMZ (don't care)
5. Packet Filters > Packet Filter Rules
   LAN – Any – Any – Accept
   RemoteLAN – Any – Any – Accept
6. VPN > IPSec
   Check and Save VPN Status
   Add an IKE connection:
   Connection name = SiteA
   Check Perfect Forward Secrecy
   Authentication Method = Secret
   Enter secret key (must be same on both sides)
   Select Encryption = 3DES
   Local WAN IP = WAN
   Local LAN = LAN
   Remote Gateway IP = RemoteWAN_IP
   Remote LAN = RemoteLAN
   Disable UID



Site B - StaticIP Addresses (Input these parameters using the RF660VPN in the branch office).

1. Domain name = site-B.com
2. Public Class C = 204.26.122.x
3. Networks & Services > Networks
   LAN: 192.168.10.0 – 255.255.255.0
   RemoteLAN: 192.168.2.0 – 255.255.255.0
   RemoteWAN_IP: 204.26.122.103 – 255.255.255.255
4. Network Setup > Interface
   Default gateway = 204.26.122.1
   Host name = RF660VPN.site-B.com
   Eth0 = LAN, 192.168.10.1, 255.255.255.0
   Eth1 = WAN, 204.26.122.3, 255.255.255.0
   Eth2 = DMZ (don't care)
5. Packet Filters > Packet Filter Rules
   LAN – Any – Any – Accept
   RemoteLAN – Any – Any – Accept

Site B - Static IP Addresses (continued)

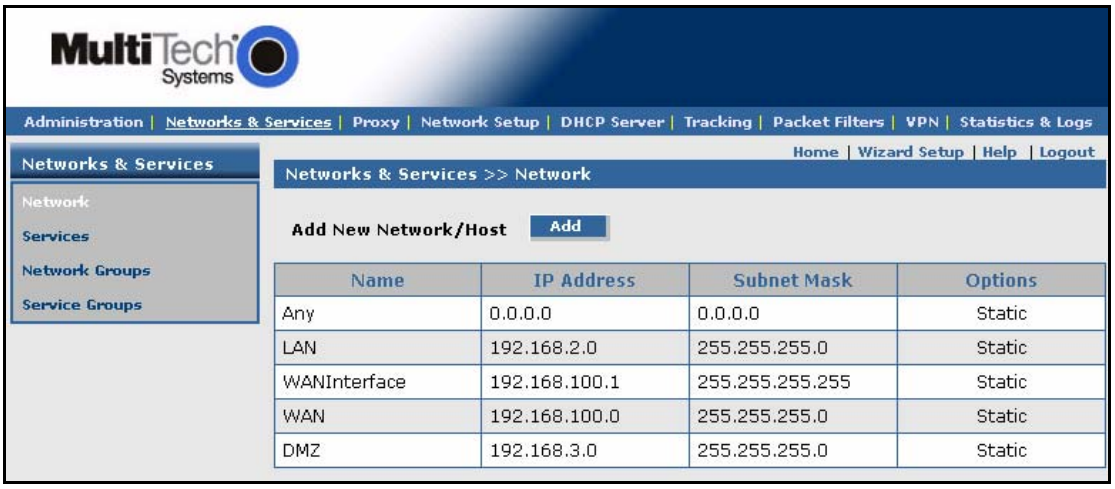
6. VPN > IPSec
   Check and Save VPN Status
   Add an IKE connection:
   Connection name = SiteB
   Check Perfect Forward Secrecy
   Authentication Method = Secret
   Enter secret key (must be the same on both sides)
   Select Encryption = 3DES
   Local WAN IP = WAN
   Local LAN = LAN
   Remote Gateway IP = RemoteWAN_IP
   Remote LAN = RemoteLAN
   Disable UID

Setup Networks & Services

Site A Configuration on the RouteFinder VPN in the Home Office

To configure your RouteFinder VPN in the home office in preparation for connection to a remote branch office, click the **Networks & Services** button on the Menu bar, and then select **Networks**. Set the following:

1. Add a network for the remote LAN port (private LAN on eth0 at the branch office). Enter the following:
   - Name = RemoteLAN
   - IP address = 192.168.10.0
   - Subnet mask = 255.255.255.0
2. Add a network for the remote WAN port (public WAN on eth1 at the branch office). Enter the following:
   - Name = RemoteWAN_IP
   - IP address = 204.26.122.3
   - Subnet mask = 255.255.255.255



Example 1 will add two network entries to the table on this screen:

Name	IP Address	Subnet Mask	Options
RemoteLAN	192.168.10.0	255.255.255.0	Edit | Delete
RemoteWAN_IP	204.26.122.3	255.255.255.255	Edit | Delete

Notes:

- **Default Entries**
  The first four entries on this screen are default entries and cannot be changed.

- **Network Data Displays on Other Screens**
  Networks added using the **Add Network/Host** on this screen will display in the *Remote Gateway IP* and *Remote LAN* dropdown boxes on the **VPN > IPSec > IKE** screen.

Set Packet Filters

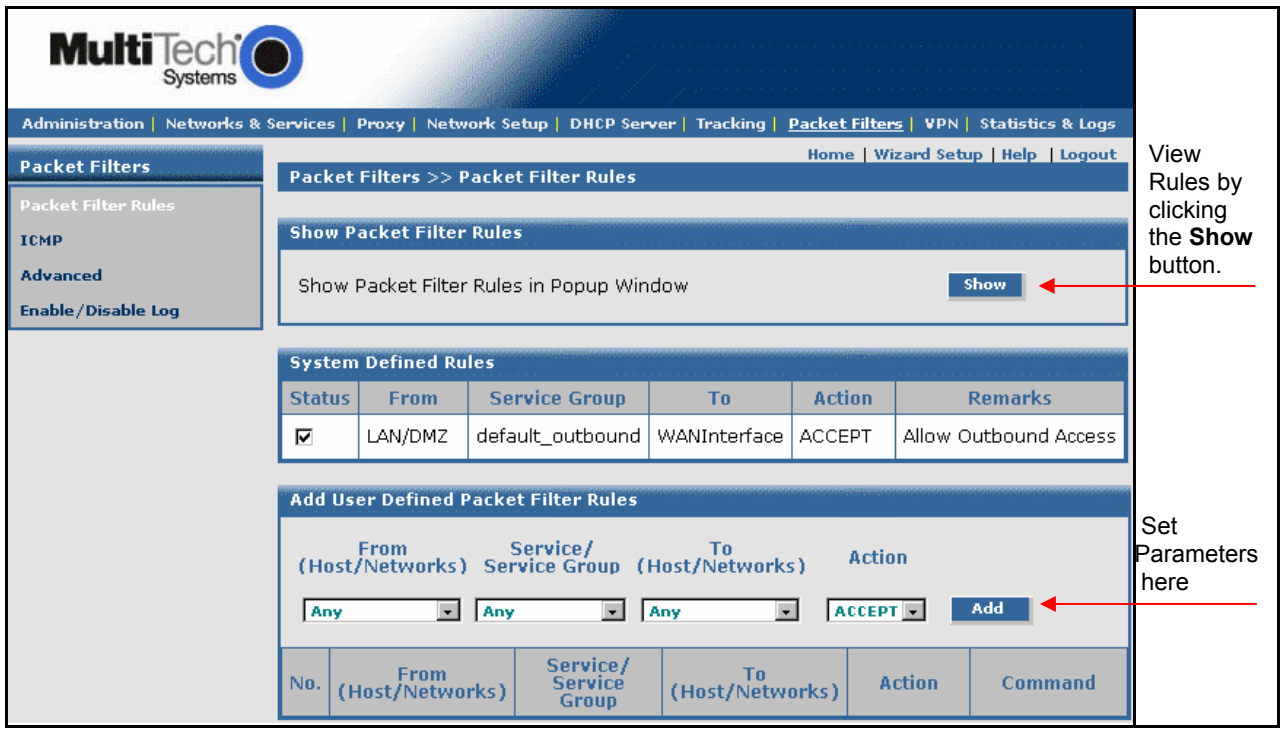
Site A Configuration: RouteFinder VPN in the Home Office

Establish remote access filtering: click on **Packet Filters > Packet Filter Rules**.

1. For the **Remote LAN** at the branch office to access the RouteFinder's LAN, select the following parameters for the Remote LAN rule:

   RemoteLAN – Any – Any – Accept

   Note: The rule **LAN – Any – Any – Accept**, which displays at the bottom of the screen, was created when you performed your initial setup using the Setup Wizard.



The rule entered in the Setup Wizard displays in this table as shown here

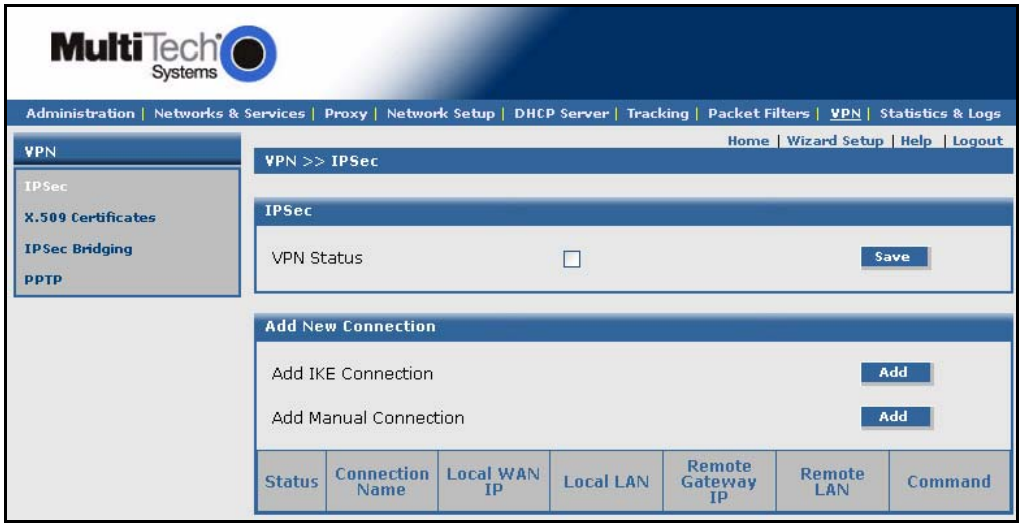
1	lan	ANY	ANY	ACCEPT	Edit|Delete|Move

Set VPN IPSec Protocol

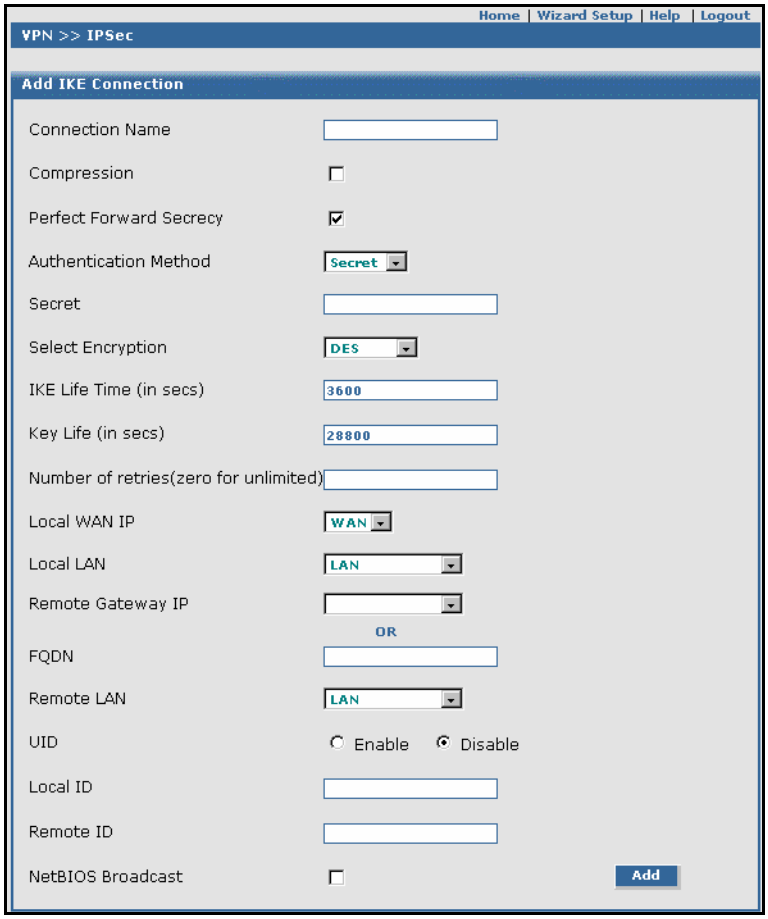
Site A Configuration: RouteFinder VPN in the Home Office

Establish an IPSec Protocol for your remote branch office access: click on **VPN > IPSec**.

1. Check the **VPN Status** box, and then click **Save**.
2. Click the **Add** button for **Add IKE Connection**.



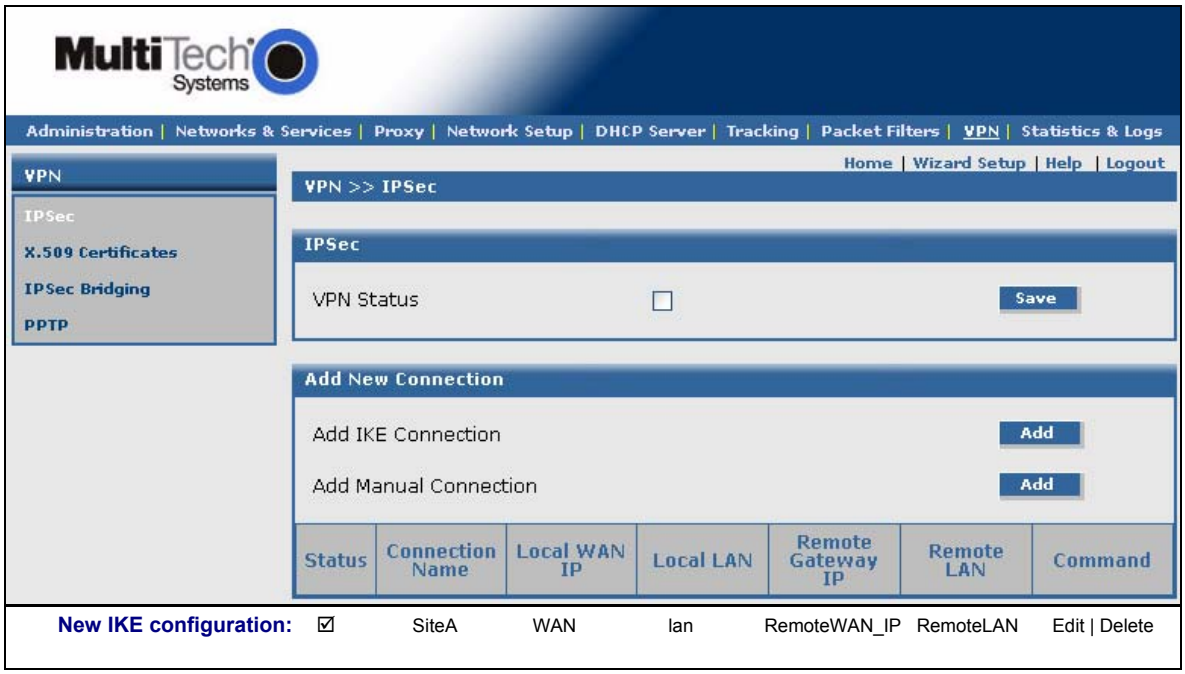
The **VPN IPSec > IKE** screen displays.



3. Enter the following information in order to establish an IPSec IKE connection.
   - Enter a **Connection name**. (Example: SiteA)
   - Place a checkmark in the box to enable **Perfect Forward Secrecy**.
   - Select **Secret** for the **Authentication Method**.
   - Enter a shared **Secret** string using alphanumeric characters. (Example: 1o2t3t4f)
   - Select **3DES** for **Select Encryption**.
   - Accept the defaults for **IKE Life Time** and **Key Life**.
   - Enter the number of retries you want the device to make in order to establish the connection. Use zero for unlimited retries.
   - Select the **Local WAN IP** and **Local LAN**. The Local WAN IP is the Public Static IP address of the WAN port (Example: WAN). The Local LAN is the private IP Network on the LAN port. (Example: LAN).
   - Select the **Remote Gateway IP** and **Remote LAN**. The Remote Gateway IP is the Public Static IP address of the WAN port at the Remote site (Example: RemoteWAN_IP). The Remote LAN is the private IP network on the LAN Port of the remote site (Example: RemoteLAN). Leave the Remote LAN blank.

     Note: FQDN is a DNS resolvable fully qualified domain name with which the right peer can be identified. When FQDN is selected, the Remote Gateway IP should be blank.
   - Disable **UID**.
4. Click **Add**.
5. The newly created IPSec IKE configuration displays at the bottom of the **VPN > IPSec** screen. To enable the connection, check the connection's **Status** box at the bottom of the screen.

   Note: Be sure that the checkmark is still in the VPN Status box at the top of the screen. Both status boxes must be checked in order for the tunnel to start.



This completes the configuration for Site A (the RouteFinder in your home office) to support a tunnel through the Internet to remote branch office.

Configuring Site B

For Site B (RouteFinder in the branch office), input the parameters listed in the table at the beginning of this section. Then follow the steps for Site A, except that now you will use the parameters for Site B listed in the example on the first page of this chapter.

Example 2 – Remote Client-to-LAN VPN Configuration

The VPN function to setup your RouteFinder so that your network allows a remote client to have access to the LAN through a secure tunnel on the Internet. Your RouteFinder includes an easy-to-use IPSec VPN client connection that transparently secures your Internet communications anytime, anywhere. This example shows the setup to allow a remote client to see a LAN, where the remote client is using SSH Sentinel.

The example shows how to configure a Remote Client-to-LAN setup. For details about this and other setups, refer to the RF660VPN Setup Examples Reference Guide, which is available on the CD included with your RouteFinder and on the Multi-Tech Systems, Inc. Web site at http://www.multitech.com/DOCUMENTS.

This setup requires:

- one RF660VPN at the home office and
- a remote client with SSH Sentinel software.

For the SSH Sentinel Client Setup at the remote site, see the separate SSH Sentinel Guide.

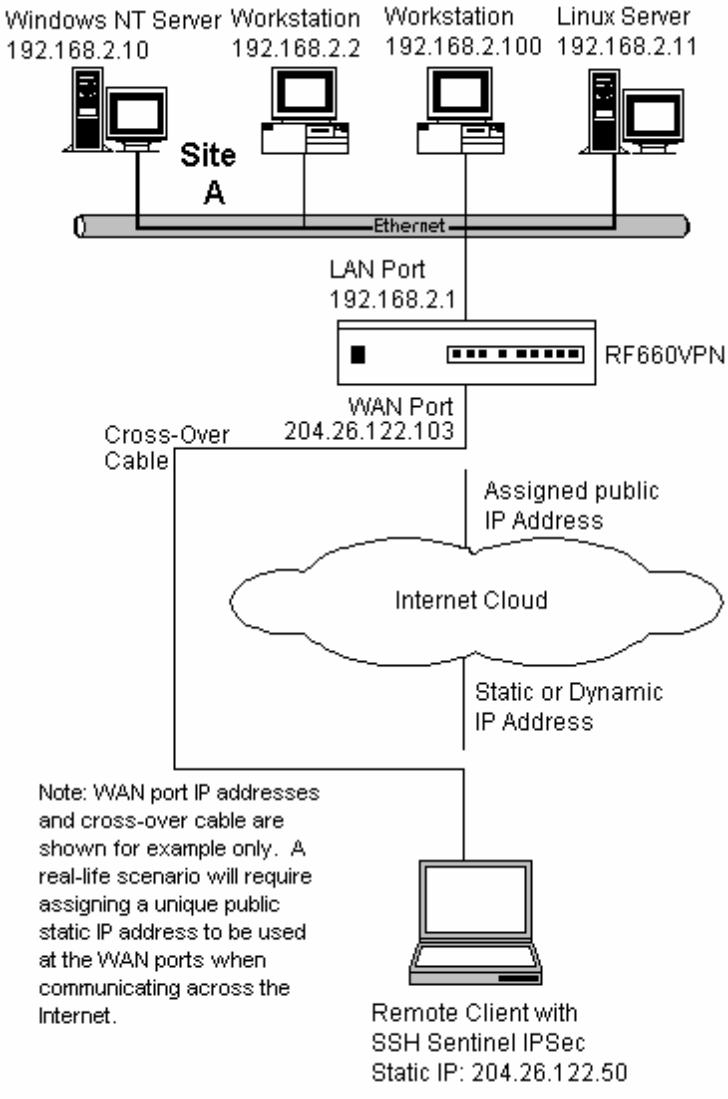
SSH Sentinel Client Accessing LAN Through RF660VPN RouteFinder (Input these parameters on the RF660VPN in the home office).

1. Domain name = Sentinel
2. Public Class C = 204.26.122.x
3. Networks & Services > Network
   LAN: 192.168.2.0 – 255.255.255.0
   Sentinel_Client: 204.26.122.50 – 255.255.255.255
4. Network Setup > Interface
   Default gateway = 204.26.122.1
   Host name = RF660VPN.Site-A.com
   Eth0 = LAN, 192,168.2.1, 255.255.255.0
   Eth1 = WAN, 204.26.122.103, 255.255.255.0
   Eth2 = DMZ (don't care)

5a. Packet Filters > Packet Filter Rules (remote client static IP)
   LAN – ANY – ANY – Accept
   Sentinel – ANY – ANY – Accept

5b. Packet Filter > Packet Filter Rules (remote client dynamic IP)
   ANY – ANY – ANY – Accept

6. VPN > IPSec
   Check and Save VPN Status
   Add an IKE connection:
   Connection name = Sentinel
   Check Perfect Forward Secrecy
   Authentication Method = Secret
   Enter secret key (must be same both sides)
   Select Encryption = 3DES
   Local Interface = WAN
   Local LAN Subnet = LAN
   Remote IP = Sentinel_Client (remote client static IP)
   Remote IP = Any (remote client dynamic IP)
   Remote Subnet = None
   UID = Disable



Example 3 – Remote Client-to-LAN Configuration Using DNAT and Aliasing

Use this procedure to configure the RF660VPN with DNAT and Aliasing. This configuration allows a Windows 2000 Remote Client to Telnet through the RF660VPN to several Windows 2000 Systems located on the LAN.

Remote Client-to-LAN Configuration Using DNAT and Aliasing Through RF660VPN

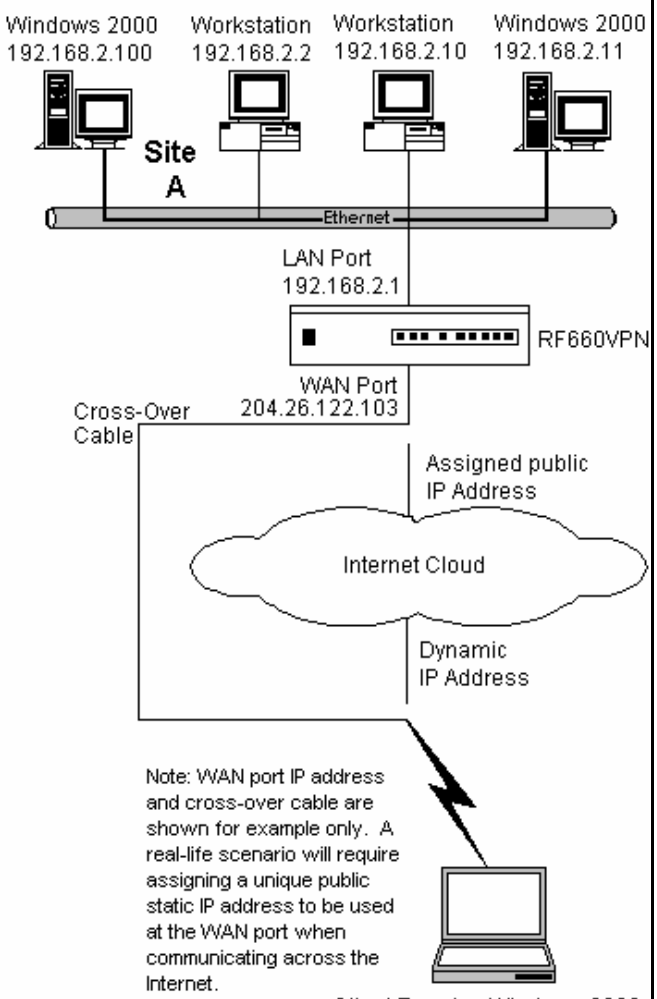
1. Networks & Services | Networks
   LAN - 192.168.2.0 - 255.255.255.0
   WANInterface - 204.26.122.103 - 255.255.255.255
   WANInterface1 - 204.26.122.104 - 255.255.255.255
   WANInterface2 - 204.26.122.105 - 255.255.255.255
   Win2k_Pro - 192.168.2.100 - 255.255.255.255
   Win2k_Server - 192.168.2.11 - 255.255.255.255

2. Network Setup | Interface
   Default gateway = 204.26.122.1
   Host name = RF660VPN.site-A.com
   eth0 = LAN, 192.168.2.1, 255.255.255.0
   eth1 = WAN, 204.26.122.103, 255.255.255.0
   eth2 = DMZ (don't care)

3. Network Setup | Interface | IP Aliases
   Eth1:0:204.26.122.104 - 255.255.255.255
   Eth1:1:204.26.122.105 - 255.255.255.255

4. Network Setup | DNAT
   WANInterface1 - Telnet - Win2k_Pro - Telnet
   WANInterface2 - Telnet - Win2k_Server - Telnet

5. Packet Filters | Packet Filter Rules
   LAN - Any - Any - ACCEPT
   Any - Telnet - Win2k_Pro - ACCEPT
   Any - Telnet - Win2k_Server - ACCEPT



Example 4 – Client-to-LAN Configuration Using PPTP Tunneling

Use this procedure to configure the RF660VPN as a PPTP server for VPN Remote Client Access (aka, PPTP Roadwarrior configuration). (**Note**: IPX and Netbeui not supported when using PPTP tunneling.)

Remote Windows 2000 Client-to-LAN Configuration Using PPTP Tunneling Through RF660VPN

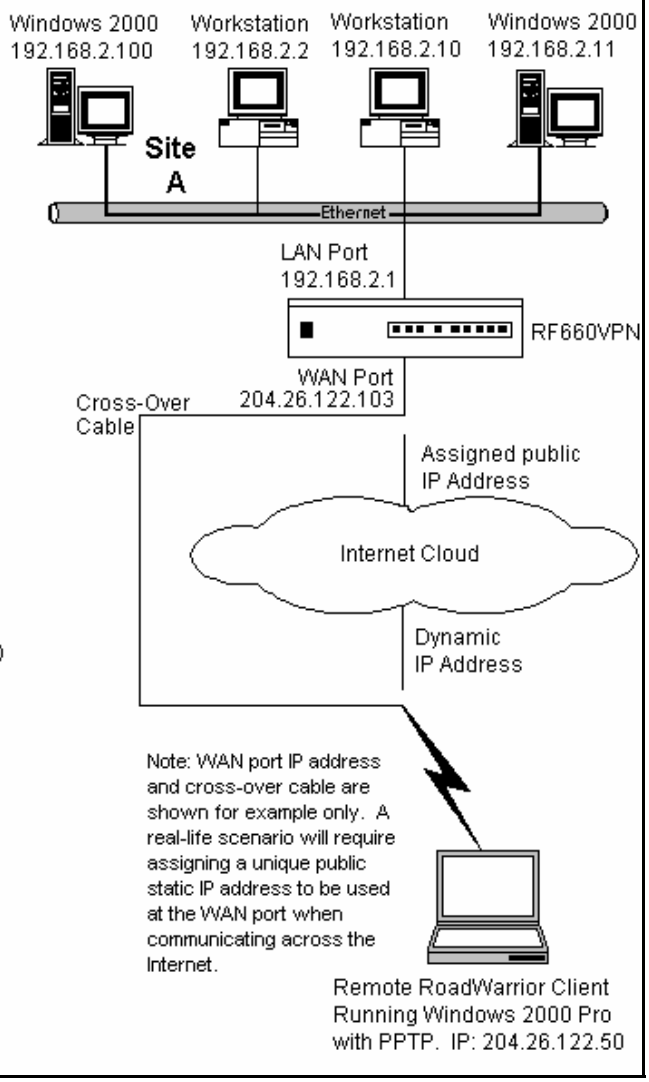
1. Networks & Services | Networks
   LAN - 192.168.2.0 - 255.255.255.0
   PPTP-Pool - 192.168.2.240 - 255.255.255.240
   (14 usable addresses)

2. Network Setup | Interface
   Default gateway = 204.26.122.1
   Host name = RF660VPN.site-A.com
   eth0 = LAN, 192.168.2.1, 255.255.255.0
   eth1 = WAN, 204.26.122.103, 255.255.255.0
   eth2 = DMZ (don't care)

3. Packet Filters | Packet Filter Rules
   LAN - Any - Any - ACCEPT

4. VPN | PPTP
   Enable PPTP Status

   Select 40 bits or 128 bits encryption strength
   Select PPTP-Pool as the remote address
   Authentication Type: Local
   Add username (roadwarrior) and password (1o2t3t4f)



Chapter 5 – URL Categorization

The Universal Resource Locator (URL) Categorization License Key allows you to set up a URL database that limits clients' access to places on the Internet by blocking sites you do not want accessed. In other words, you can deny users access to various categories of Web sites you select.

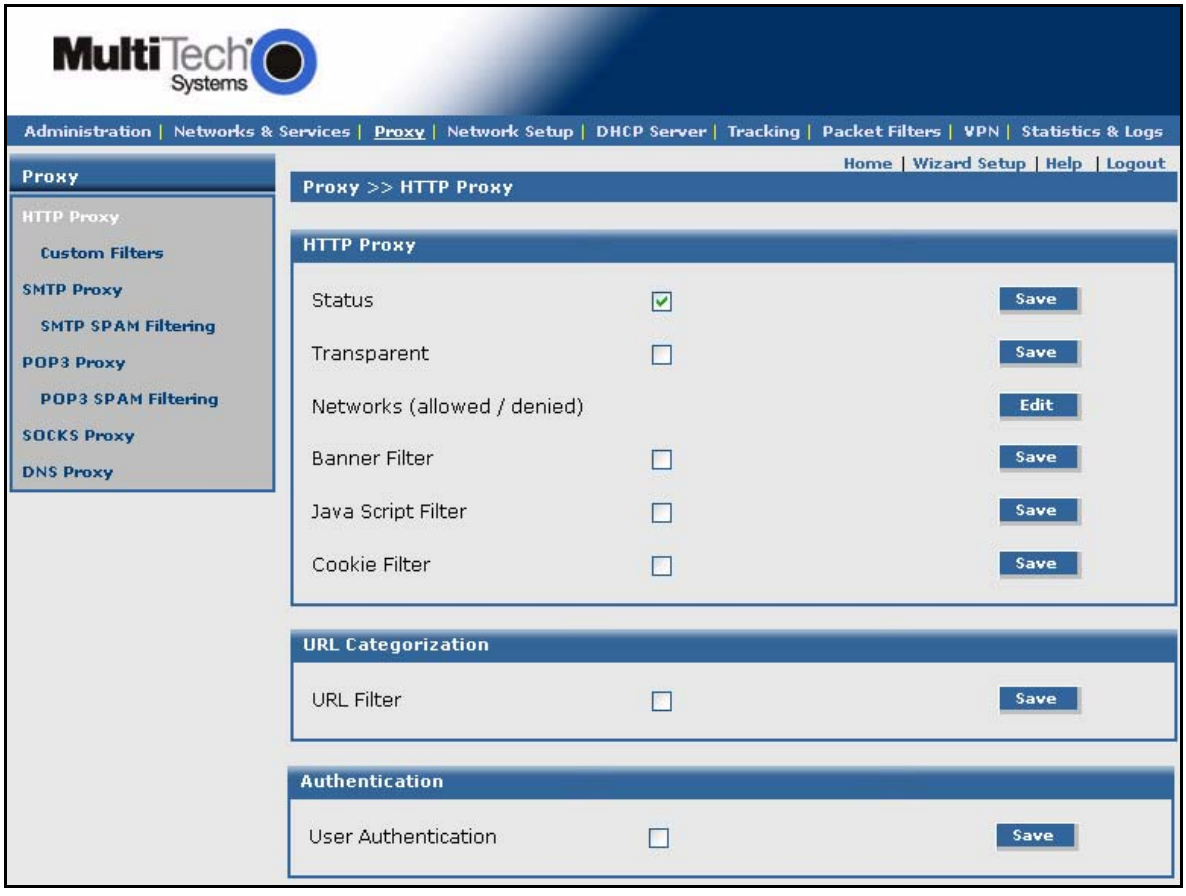
Important Settings

- Client access to the Internet works in conjunction with the HTTP proxy running in **transparent mode**.
- The RouteFinder must be connected to the Internet for the URL License to be activated.

Setting Up HTTP Proxy and URL Filtering

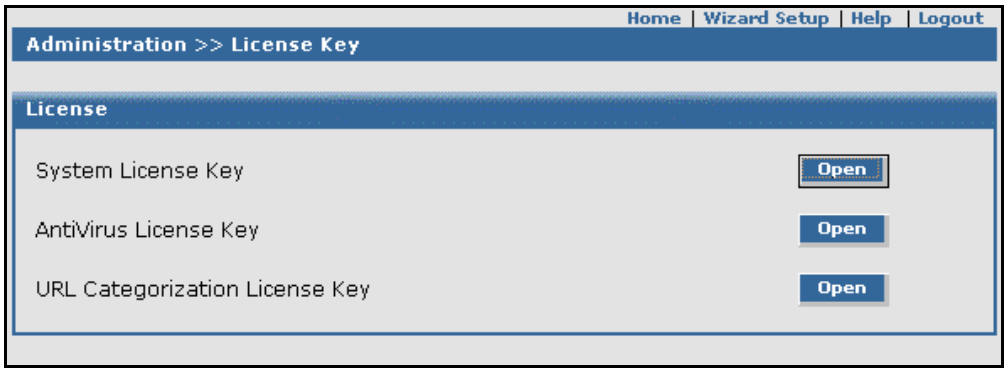
- Click **Proxy** from the Menu bar. The **HTTP Proxy** screen displays.
- Check **Status** box and click **Save**.

  Important: The **Status** box must be checked before you can enter and activate your URL Categorization License Key.

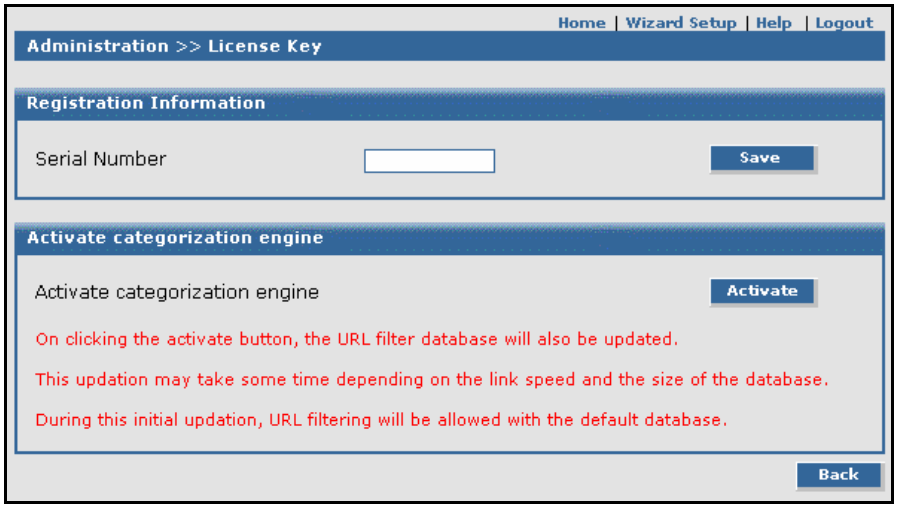


Note About URL License Key: The URL License number must be entered on the **Administration > License Key** screen before the URL Categorization section of this screen displays. The key number is located on the bottom of the RouteFinder chassis and on the front of the Quick Start Guide.

- Go to the **Administration > License Key** screen to enter your URL License Key. This is a required in order to use this feature.
- Click the **Open** button across from **URL Categorization License Key**.

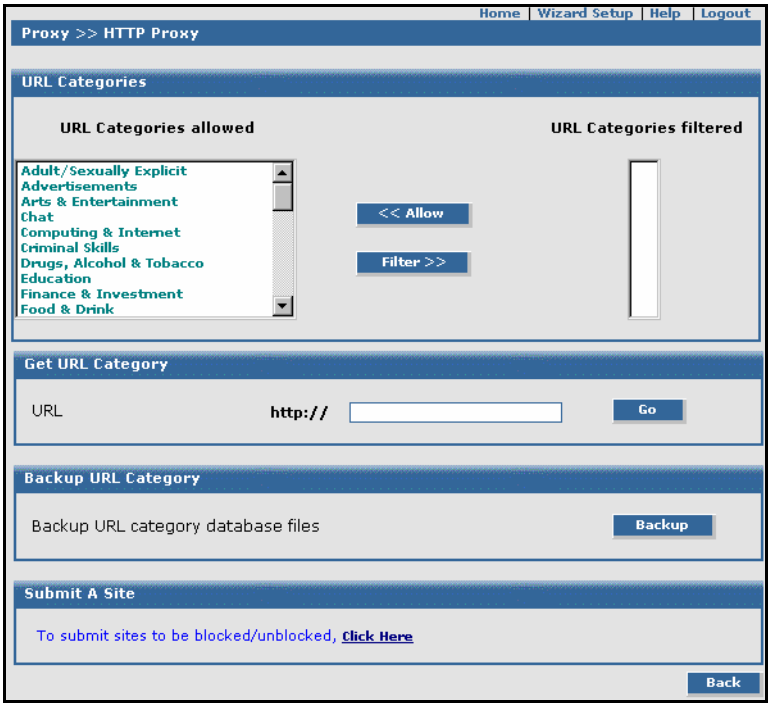


The **Administration > License Key > URL Categorization** screen displays:



- Using upper case letters, enter the 11-digit serial number of the URL License Key and click the **Save** button. **IMPORTANT:** It is important that the serial number be entered in upper case.
- Click the **Activate** button. The categorization engine's expiration date and time display.
- Return to the **Proxy > HTTP Proxy** screen to set your URL filtering categories. See the screen on the previous page.
- Check the **Transparent** box and click **Save**.
- Check the **URL Filter** box and click **Save**. Once you click Save, two additional fields display: **URL Categories** and **Networks / Hosts to bypass URL Filtering.**
- Click **Edit** for **URL Categories (Allowed/Filtered)**. Not shown on the screen example above.

- The **URL Categories** screen displays. You can use this screen to allow or block Web sites from users.



  - Use the **Allow** and **Filter** buttons to move a URL Category from the *URL Categories Allowed* list to the *URL Categories Filtered* or from *Filtered* to *Allowed*.
  - When you have established your filtered and allowed categories, click the **Backup** button to create a backup of your URL category database files.
  - When you are finished organizing the categories, click the **Back** button to exit the screen.

How to Test Web Sites for Blocking

You can test specific Web sites to see if the URL has been blocked (use **Get URL Category** to perform this test) or submit a site to be blocked or unblocked by the SurfControl software, which sets up the categories stored in this software.

How to Test the Filtering

Type a URL in the **http://** box and click the **Go** button. This will test the URL to see if it is allowed or blocked.

Note: You can also test a site through your browser by entering a Web address that you feel should be blocked by the filter through one of the categories you had chosen or a category preset by the URL software. For instance, if you selected the **Finance and Investment** category to be filtered, try to access www.etrade.com. This site should be blocked. A message displays under the URL address stating the status of this Web site.

Important: The sites listed in the **Favorites** box of the browser will not be blocked unless the cache is emptied in the browser.

Establishing Filtering Rules for Networks and Hosts

Return to the **Proxy > HTTP Proxy** screen by clicking the **Back** button on the **Proxy > HTTP Proxy > URL Categorization** screen.

- Click the **Edit** button for **Networks / Hosts to bypass URL Filtering**. The **Networks / Hosts to bypass URL Filtering** screen displays. You can use this screen to allow or block Web sites from Networks / Hosts.
- Click the **Add** button to move a network/host name into the **Network/Hosts to Bypass URL Filtering** box.
- If you decide that you do not want one or more of the networks/hosts bypassing the filter, select the name and click the **Delete** button. The name moves back into the **Available Networks/Host** box.

Submitting a Site to SurfControl for Reconsideration

Filtered categories are setup and controlled by the *SurfControl* software that is built into your RouteFinder VPN. There may be a category you would like to see added or deleted. You can submit sites to be blocked or unblocked. Click the words **Click Here** to open a proposal screen and send it to SurfControl.

Chapter 6 – RouteFinder Software

This chapter describes each screen and its function in the RouteFinder VPN software. The aim of the administrator in setting the options in the software should be to let as little as possible and as much as necessary through the RouteFinder VPN, for both incoming as well as outgoing connections.

Note: If you have not done so already, plan your network and decide which computers are to have access to which services. This simplifies the configuration and saves you a lot of time that you would otherwise need for corrections and adjustments.

Menu Bar

The Menu bar will provide the organization of this chapter.

Important Note About Logout

Logout Closes the Software Program and Saves Settings

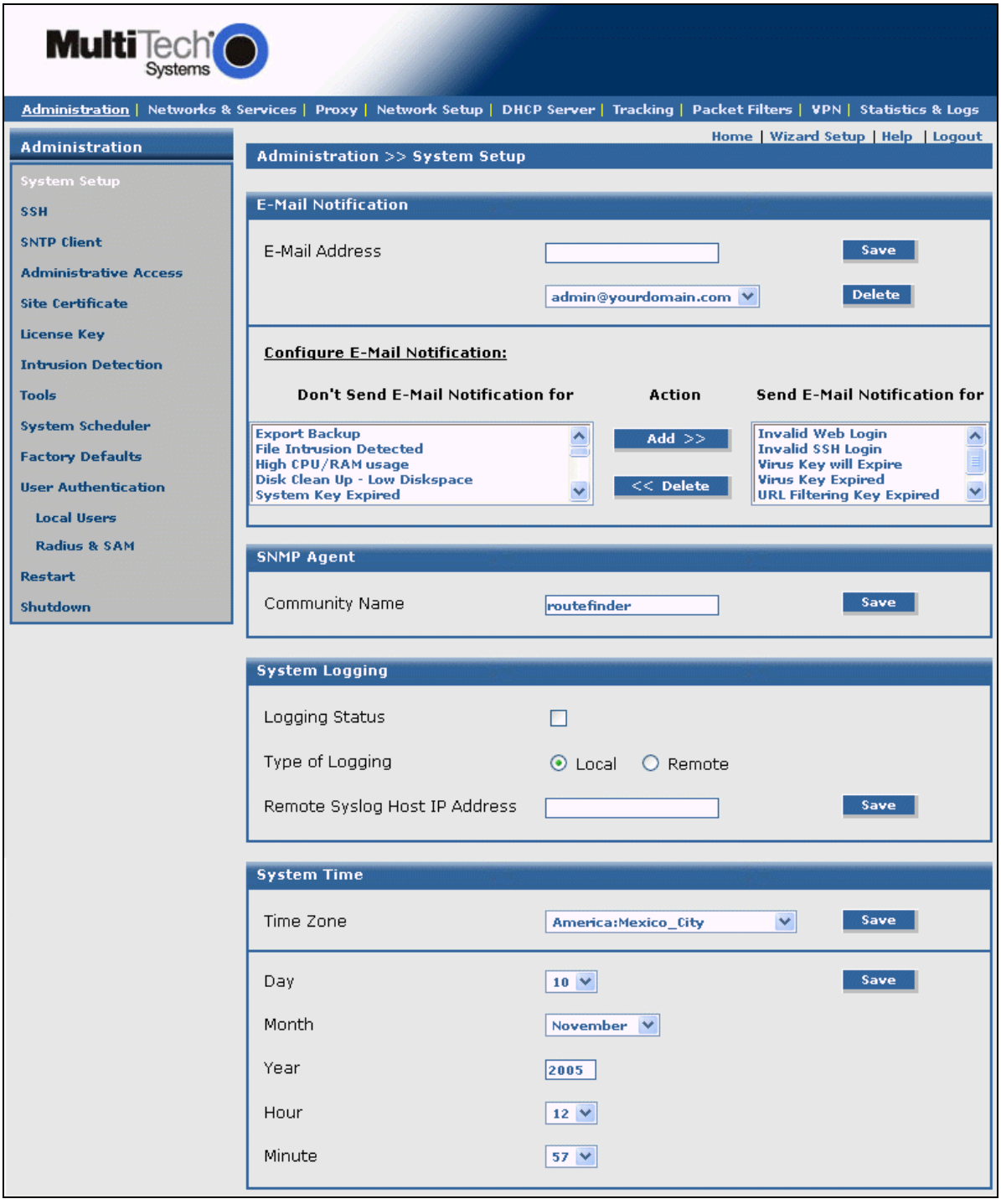
The best way to exit WebAdmin is to choose Logout. This will save all your current settings. The browser connection is terminated and you are returned to the **Login** screen. Note that clicking the browser's **Back** button will not effectively return you to the previous menu or directory at this point.

If you close the browser while configuring the RouteFinder, the last session stays active until the end of the time-out, and no new administrator can log in. The timeout period is set at **Administration > Administrative Access > Time Before Automatic Disconnect**.

Administration

Administration › System Setup

In the **Administration** part of the software, you can set the RouteFinder general system-based parameters.
System Setup includes general system parameters such as the Administrator's email address, SNMP Agent, System Logging, Remote Syslog Host, and the System Time.



Email Notification

Email Address: Enter the **Email Address** of the administrator who will receive the email notifications. Click **Save**. You can delete the entry and change it at any time, if desired.

At least one email address must be entered in this field.

Configure Email Notifications the RouteFinder VPN Will Send

Select the types of notifications that you want sent. Click the **Add** button. The name will then appear in the **Send Email Notification For** box. You can remove a type by clicking the **Delete** button. The name will than move back to the **Don't Send Email Notification For** box.

1. Export Backup (the backup file will be attached)
2. File Intrusion Detection (File Integrity Checks and Network Intrusions)
3. High CPU/RAM Usage (Hard disk usage exceeding 70%)
4. Disk Clean Up – Low Diskspace
5. System Key Expired (10 days before expiry)
6. Invalid Web Login
7. Invalid SSH Login
8. Port Intrusion Detected
9. PPP backup link down
10. PPP backup link up
11. URL Filtering Server Error
12. Auto System Update
13. Virus Key Will Expire
14. Virus Key Has Expired
15. Virus Database Updated
16. URL Filtering Key Expired
17. URL Filtering Key Will Expire (10 days, 2 days, and 1 day before expiry)
18. URL Filtering Categories Updated
19. URL Categories Update Failed
20. Bayesian Database Has Reached Maximum
21. POP3 Virus Mail
22. HTTP Access Deny Reports

The mail settings are saved in the server configuration. The first email ID in the list should be the Administrator's ID, so that when the first ID is added or deleted, the session is terminated and the Web server restarted.

SNMP Agent – Community Name

Type the community name for the SNMP Agent.

System Logging

Check the **Logging Status** box to activate and enable the host to receive log messages from other machines.

Select the type of logging, either **Local** or **Remote**.

Then type the IP address of the **Remote Syslog Host** to which all log messages from the RouteFinder will be forwarded. Click **Save**. The IP address is a required parameter.

On the remote host, syslog should be invoked with the "-r" option to enable the host to receive log messages from other machines. This is especially recommended if you want to collect the log files of several systems on one host. The default setting is 'off'.

System Time

Select the system time, time zone, and current date.

Note: It is not recommended that you change from summertime to wintertime and back. We suggest entering Greenwich Mean Time (GMT), regardless of your global position, especially if you plan to operate Virtual Private Networks across different time zones. Changing the system time can lead to the following time-warp effects:

Forward time adjustment (winter to summertime)

- The time-out for the **Web Admin** has expired and your session is not valid anymore.
- Log information for some time periods may be missing in the time-based reports.
- Most diagrams show this time period as a straight line at the height of the old value.
- All the values for Accounting in this time period are 0.

Backward time adjustment (summer to wintertime)

- The time-based reports already contain log information for the corresponding time period which, as far as the system is concerned, comes from the future: this information is not overwritten, but is retained.
- The writing of the log files is continued from the point of time before the setback time is reached.
- Most diagrams show the values of this time period as compressed.
- The already-recorded data (from the future) retain their validity for the Accounting function.
- The accounting files are continued when the setback time is reached again. Therefore, it is recommended that the time should only be set once during initial configuration and later should only be slightly adjusted. No adjustments from wintertime to summertime should be made, especially if the collected reporting and accounting information is to be further processed.

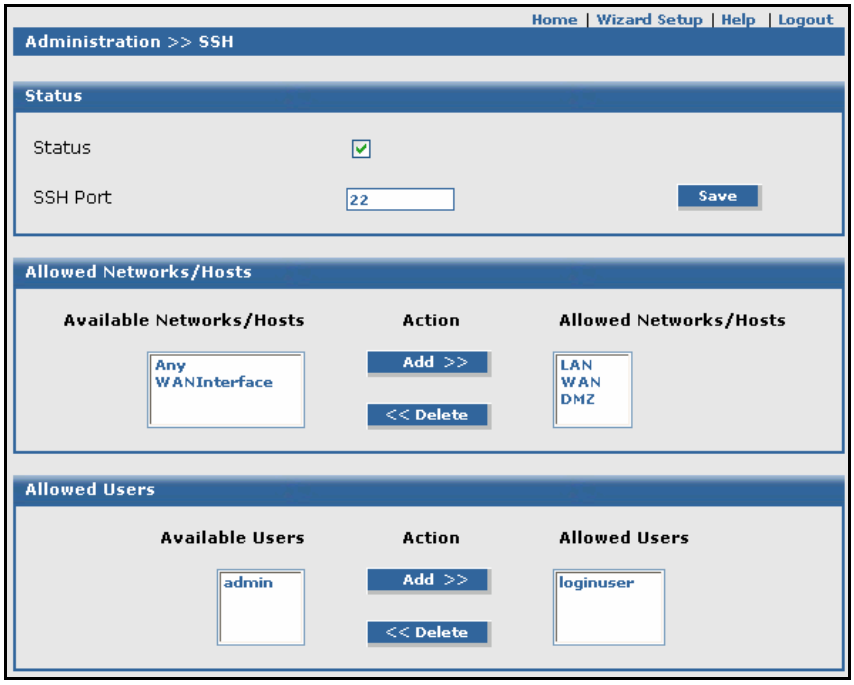
Administration › SSH

What Is SSH

SSH (Secure Shell) is a program to log into another computer over a network to execute commands in a remote machine and to move files from one machine to another. It provides strong authentication and secure communications over an insecure network. It is intended as a replacement for **rlogin**, **rsh**, and **rcp**. The SSH configuration provides access to the firewall using SSH channel. SSH is a text-oriented interface suitable only for the experienced administrators. Access via SSH is encrypted and, therefore, impossible for outside users to tap into it.

Prerequisites

- For access via SSH**,** you need an SSH Client, which most Linux systems already include. For MS Windows, the program **PuTTY** is recommended as an SSH client.
- To log into the RouteFinder with Secure Shell (SSH, Port 22), use the **login user** account and the appropriate password that was set up during installation. Remember to change your password regularly!
- Networks allowed to access the RouteFinder using SSH are added on this screen; other networks can be defined on the **Networks & Services > Networks screen**.



Status and SSH Port

Initially, this screen displays with **Status** as the only prompt. Once **Status** is checked and you click **Save**, SSH is enabled and the other options display. The TCP port number for the SSH session is specified in the SSH Port Number field; the default is Port 22.

SSH requires name resolution for the access protocol; otherwise, a time-out occurs with the SSH registration. This time-out takes about one minute. During this time it seems as if the connection is frozen or that it can't be established. After that, the connection returns to normal without any further delay.

Allowed Networks

Networks allowed to access the RouteFinder through SSH can be added and deleted here. The default **Any** in **Allowed Networks** ensures a smooth installation and allows everyone to access SSH service.

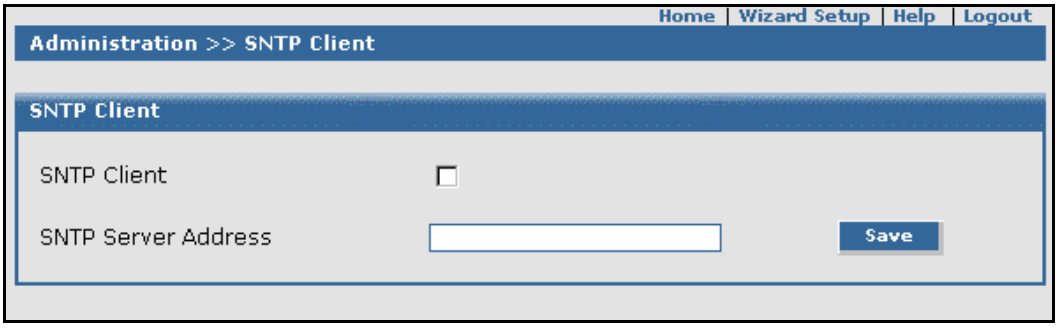
Caution: While the default setting (**Any**) allows everyone to access the SSH service, we recommend that you restrict access to the SSH service for security reasons. You should delete access from all other networks! When deleting a network, the program checks whether you are still able to access **Administration > Administrative Access** from your active IP address after the deleting procedure. If this is no longer possible, the process is not carried out. This check is carried out for the security of the administrator and will ensure that the administrator cannot become locked out accidentally. After completing the adjustments, it is a good idea to disable SSH access again for security reasons.

Allowed Users

Users allowed to access the RouteFinder through SSH can be added and deleted here. Highlight the Users you want to have access to SSH service and click the **Add** button. Users can be deleted from this list at any time.

Administration › SNTP Client

SNTP (Simple Network Time Protocol) is an internet protocol used to synchronize the clocks of computers on the network. Clicking the SNTP Client check box enables the firewall to act as a SNTP client.



SNTP Client

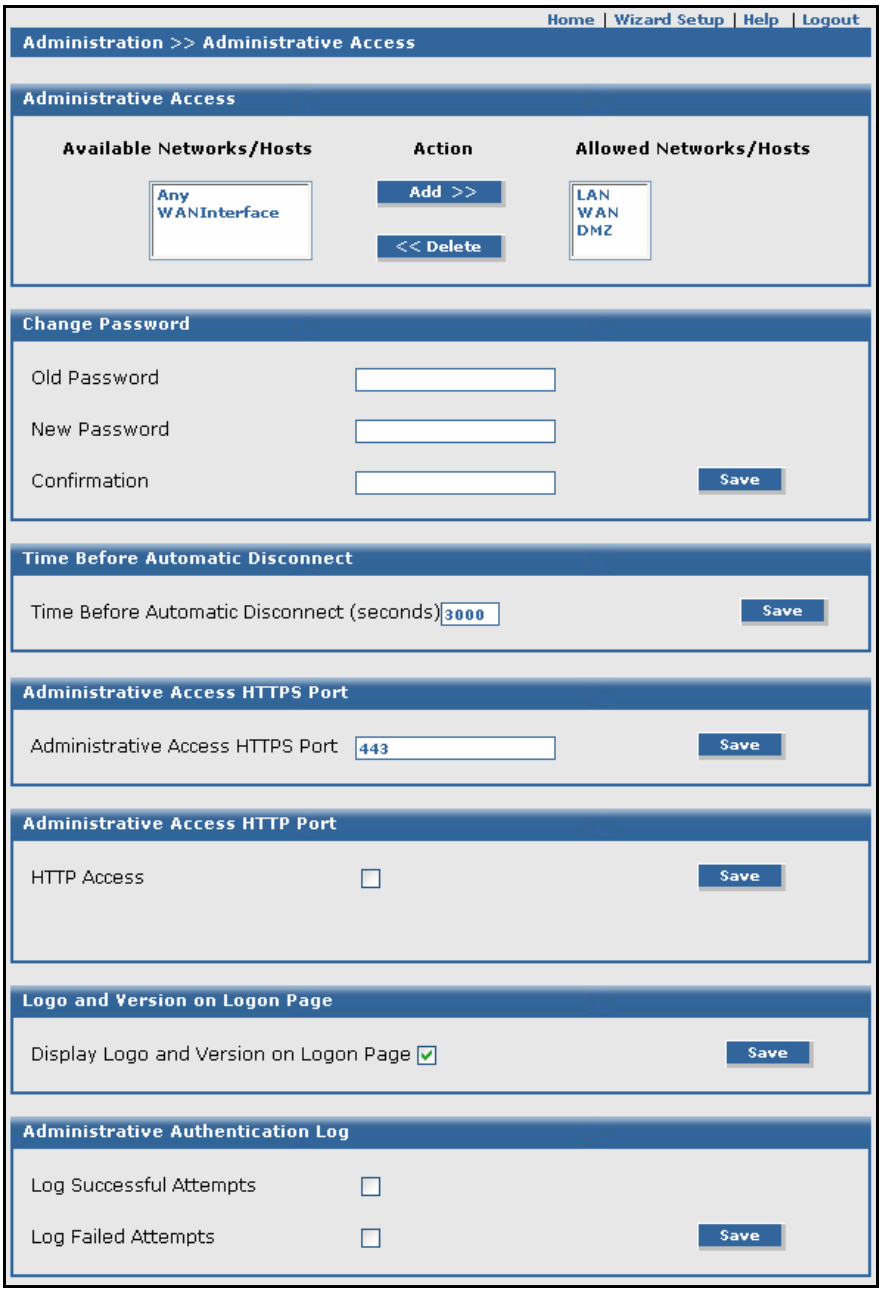
Check the SNTP Client box to activate SNTP Client.

SNTP Server Address

Enter the IP address of the SNTP Server for which the firewall will contact to synchronize its clock. Then click the **Save** button.

Administration › Administrative Access

The networks and hosts that are allowed to have administrative access are selected on this screen. This is a good way to regulate access to the configuration tools.



Administrative Access - Available Networks and Allowed Network

Select the networks/hosts that will be allowed administrative access. Note that the selection box list will include those networks you enter under **Networks & Services > Networks**.

You can change access by moving network/hosts names from the **Available** list to/from the **Allowed** list. The RouteFinder will display an ERROR message if you try to delete access to a network that would cause you to lock yourself out.

Allowed Networks

The default **Any** has been entered here for ease of installation. **ANY** allows administrative access from everywhere once a valid password is provided.

Caution: As soon as you can limit the location from which the RouteFinder is to be administered (e.g., your IP address in the internal network), replace the entry **ANY** in the selection menu with a smaller network. The safest approach is to have only one administrative PC given access to the RouteFinder. You can do this by defining a network with the address of a single computer from the **Networks and Services > Networks** screen.

Change Password

You should change the password immediately after initial installation and configuration, and also change it regularly thereafter. To change the password, enter the existing password in the Old Password field, enter the new password into the New Password field, and confirm your new password by re-entering it into the Confirmation entry field.

Caution: Use secure passwords! For example, your name spelled backwards is not secure enough; something like **xfT35$4** is better.

Time Before Automatic Disconnect

An automatic inactivity disconnection interval is implemented for security purposes. In the **Time Before Automatic Disconnect** entry field**,** enter the desired time span (in seconds) after which you will be automatically disconnected from the software program if no operations take place.

After the initial installation, the default setting is 3000 seconds. The smallest possible setting is 60 seconds. If you close the browser in the middle of an open configuration session without closing via Exit, the last session stays active until the end of the time-out and no new administrator can log in.

If using SSH, you can manually remove the active session if you log into the RouteFinder as login user via **SSH**. With the command SU, you become a root user and can then interrupt the current connection with rm -f /tmp/wfelock**.**

Administrative Access HTTPS Port

This field is used for setting the HTTPS port for Web administration. After setting the HTTPS port, the connection is terminated. The browser settings have to be changed for the new port number before starting the next session.

By default, port 443 is configured for HTTPS sessions. The value of the port number should lie between 1 and 65535. Well known ports and ports already used by the firewall are not allowed.

If you want to use the HTTPS service for other purposes (e.g., a diversion with **DNAT**), you must enter a different TCP port for the interface here. Possible values are 1-65535, but remember that certain ports are reserved for other services. We suggest you use ports 440-450. To have Administrative Access after the change, you must append the port to the IP address of the ROUTEFINDER separated by a colon (e.g., https://192.168.0.1:445).

Administrative Access HTTP Port

Check this box if you want to use HTTP to access the RouteFinder's software. This is less secure, but it is faster when performing administrative tasks. Click **Save**.

Logo and Version on Logon Page

Check this box if you want the logo and version number to display on the logon page. Click **Save**.

Administrative Authentication Log

Log Successful Attempts

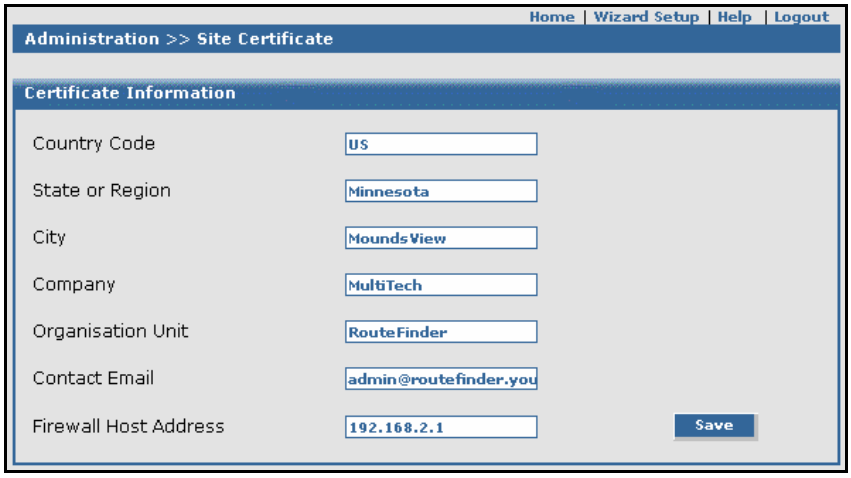
If you check this box, the successful login attempts at the RouteFinder's administrative access interface will be recorded and displayed on the **Statistics & Logs > Administrative Authentication** screen.

Log Failed Attempts

If you check this box, the failed login attempts at the RouteFinder's administrative access interface will be recorded and displayed on the **Statistics & Logs > Administrative Authentication** screen.

Administration › Site Certificate

Public keys are used as the encryption algorithm for security systems. For the validity of public keys, certificates are issued by a Certificate Authority. The Certificate Authority certifies that the person or the entity is authenticated and that the present public key belongs to that same person or entity. As the certificate contains values such as the name of the owner, the validity period, the issuing authority, and a stamp with a signature of the authority, it is seen as a digital pass. On this screen, you enter server certificate information, which the firewall needs to authenticate itself to your browser. After saving the settings, the browser's security information settings have to be cleared.



Enter the Certificate Information

Country Code – Use the default (United States) or change to the country of operation.

State or Region – Type the state, province, region, etc. of operation.

City – Type the city name.

Company – Type the company name.

Organization Unit – Type the organizational unit (e.g., Sales & Marketing).

Contact Email – Type the email address of the contact for RouteFinder certificate data (e.g., the RouteFinder administrator) over the default (myname@mydomain.com).

Firewall Host Address – Enter the RouteFinder's host address. Use the same address that you will use to open the Administration Access interface. It can be one of the RouteFinder IP addresses.

- ***Example:*** If you access Administration Access with https://192.168.10.1, the Host Address must also be **192.168.10.1**. If you access Administration Access with a DNS host name (e.g., https://MultiAccess Communications Server.mydomain.com), then use this name instead.
- ***Note:*** The Host Address field MUST match the host Address or IP Address that you use in your browser to open Administration Access.

Click Save

The browser will reconnect to the VPN. At the security Alert screen, click **View Certificate.** Then click **Install Certificate** if you have not previously installed it:

Install the Certificate into the Trusted Root Certification Authorities Store

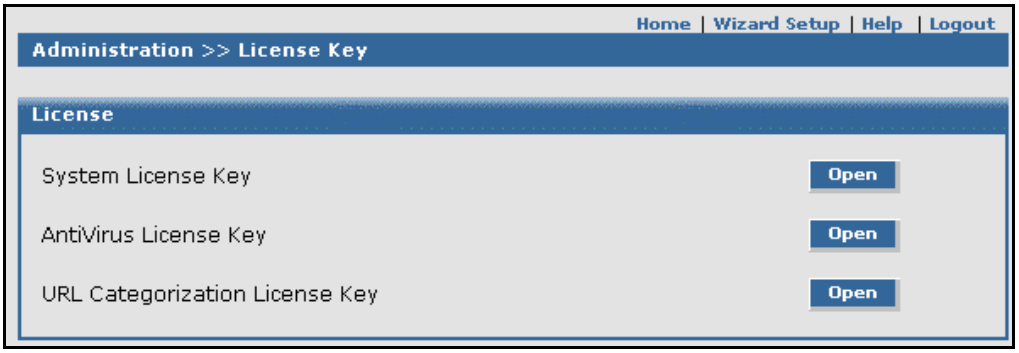
1. When the first screen displays, click the **Install Certificate** button.
2. On the Welcome to Certificate Import Wizard screen, click the **Next** button.
3. On the Certificate Manager Import Wizard screen, click **Next**. You can elect to have the certificate automatically placed into a directory or you can Browse and choose your own directory. If you elect to place all certificates into a selected location, follow the on-screen prompts for Select Certificate Store, Physical Stores, and Root Stores.
4. When the certificate has been added to the Root Store, the Completing the Certificate Manager Import Wizard displays. Click **Finish**.

Administration › License Key

The system license key, virus scanner license key, and the URL Categorization engine license key can be configured from this screen.

Notes:

- Each RouteFinder ships with a unique individual system license key. It is a 20-digit code that is provided on the RouteFinder CD.
- Each RouteFinder ships with a URL Categorization License Key. It is provided on the RouteFinder CD.
- The AntiVirus key can be purchased from Multi-Tech Sales Support.



License

Click the **Open** button for the desired license key. The **Enter License Key** screen displays.

System License Key

Enter the license key number assigned to your RouteFinder and click **Save**. When you have entered the License Key accurately, the Enter System License Key screen is re-displayed.

Important:

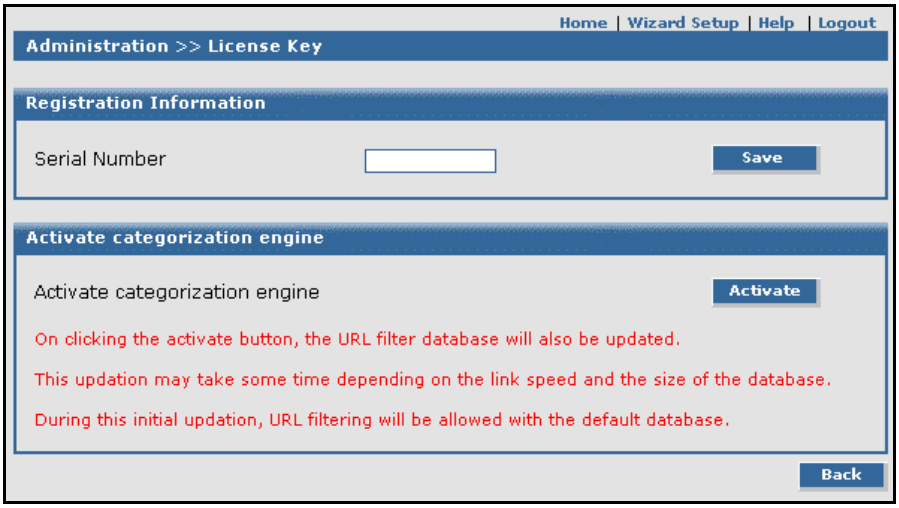
- The license key number is a 20-digit alphanumeric entry; **the letters must all be in upper case**.
- If you enter your license key number incorrectly, the message ***Error: License is invalid*** is displayed. Check the license key number and re-enter it. One common entry error is mistaking a 0 (zero) for an o (the letter O). Another entry error is entering lower case letters or symbols.
- The License Key number is tied to and tracked with your RouteFinder's serial number.
- Whenever you require additional licenses, you must first provide Multi-Tech with your current License Key and serial number information in order for us to update your RouteFinder.
- With a valid License Key, you are entitled to use Multi-Tech's Update service and support.

AntiVirus License Key

The AntiVirus license key can be purchased from Multi-Tech sales support.

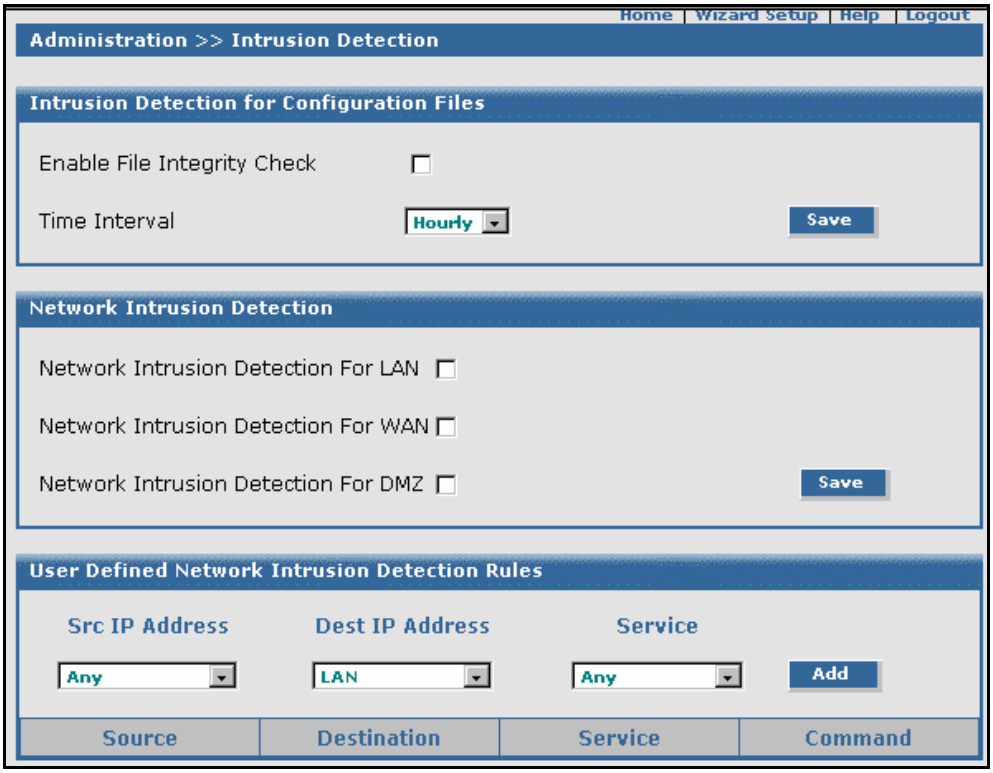
URL Categorization Key

This license key is included with your RouteFinder when it ships, but you must enter the license key to activate the feature. The key number is included on the RouteFinder CD.



Administration › Intrusion Detection

The Intrusion Detection mechanism notifies the administrator if there has been any tampering with the files on the server.



Intrusion Detection

Enable File Integrity Check – Check the box to enable File Integrity Checking.

Time Interval – Select the amount of time you would like the system to conduct this check. Options are every 5 Minutes, Hourly, or Daily. Then click the **Save** button.

Network Intrusion Detection

This allows the user to detect attacks on the network. In the event that port scans are carried out by hackers who look for a secure network with weak spots. When this feature is enabled, it informs the administrator by email as soon as the attack has been logged. The administrator can decide what actions are to be taken. By default, DOS attack, minimum fragmentation checks, port scans, DNS attacks, bad packets, overflows, chat accesses, Web attacks will be detected; and then the administrator is informed. Apart from the above, the user can configure user-defined rules for intrusion detection.

Enable Network Intrusion Detection for LAN – Check the box to enable Network Intrusion Detection for the LAN. Then click the **Save** button.

Enable Network Intrusion Detection for WAN – Check the box to enable Network Intrusion Detection for the WAN. Then click the **Save** button.

Enable Network Intrusion Detection for DMZ – Check the box to enable Network Intrusion Detection for the DMZ. Then click the **Save** button.

User-Defined Network Intrusion Detection Rules

SRC IP Address

This selection allows you to choose the network from which the information packet must be sent for the rule to match. Network groups can also be selected. The ANY option matches all IP addresses; it does not matter whether they are officially assigned addresses or private addresses. These Networks or groups must be predefined in the Networks menu.

Destination IP Address

This selection allows you to choose the network to which the information packet must be sent for the rule to match. Network groups can also be selected. These network clients or groups must have been previously defined in the Networks menu.

Protocol

This selection allows you to choose the corresponding service. The service must have been previously defined in the Services menu. Select intrusion detection rules from the following dropdown list boxes:

Add

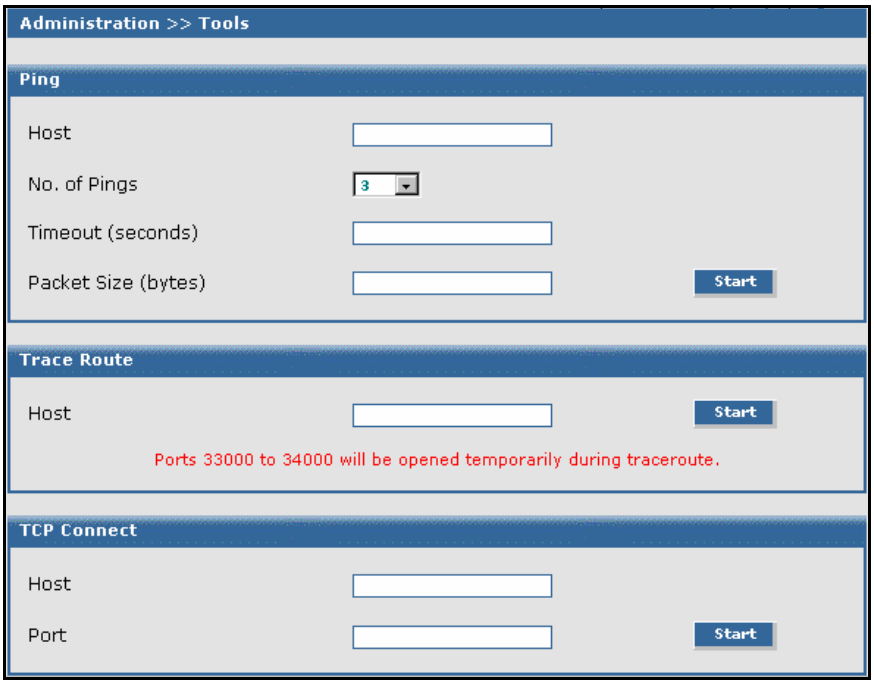
After the rules are defined/selected, click the **Add** button. The commands can be deleted by clicking **Delete** under the Command option.

Administration › Tools

There are three tools that can help you test the network connections and RouteFinder functionality. Ping and Trace Route test the network connections on the IP level. TCP Connect tests TCP services for availability.

Notes:

1. For these tools to function, the ICMP on firewall function in **Packet Filter > ICMP** must be enabled.
2. For the Name Resolution function, enable the DNS proxy function in **Proxy > DNS**. To use the Name Resolution function, enable a name server in the menu (item) Proxy > Name Server. When the Name Server is enabled, the IP addresses of the reply packets will be converted into valid names.



PING

Ping is an acronym for Packet Internet Groper. The PING utility is used as a diagnostic tool to determine if a communication path exists between two devices on the network. The utility sends a packet to the specified address and then waits for a reply. PING is used primarily to troubleshoot Internet connections, but it can be used to test the connection between any devices using the TCP/IP protocol.

If you PING an IP address, the PING utility will send four packets and stop.

If you add a -t to the end of the command, the PING utility will send packets continuously.

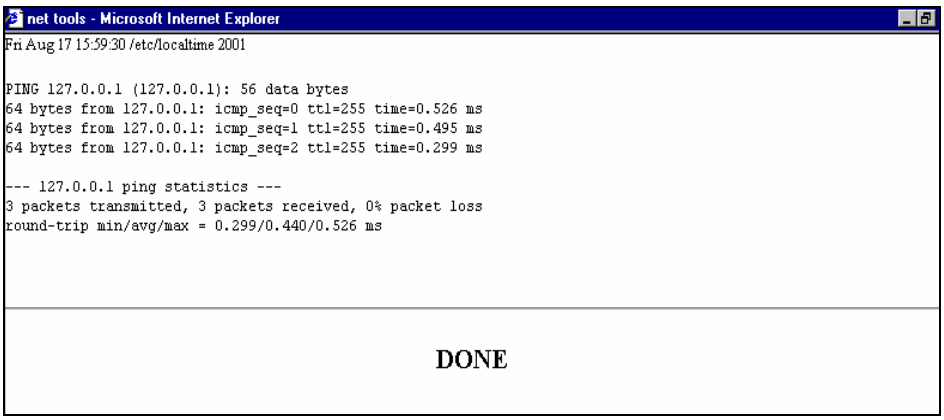
Host – Specify the IP address or name of the other computer for which connectivity is to be checked.

Number of PINGS – Select the number of pings. You can choose 3 (the default), 10 or 100 pings. Enter the IP address or the name into the Host entry field (e.g., port **25** for SMTP).

Timeout – Specify the time that packets can exist.

Packet Size – Specify the number of data bytes to be sent.

Start – After clicking the Start button, a new browser window opens with the PING statistics accumulating. "Close the PING Statistics Window to A Sample" PING log is shown below.



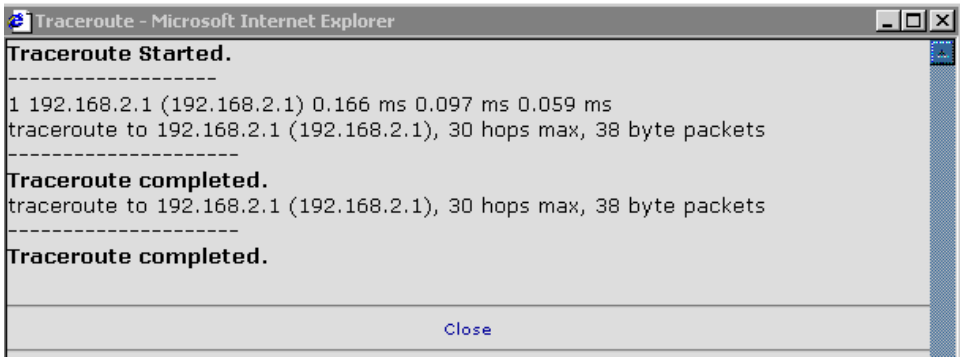
Trace Route

Trace Route is a tool for finding errors in the network routing. It lists each router's addresses on the way to remote systems. If the path for the data packets is temporarily unavailable, the interruption is indicated by asterisks (*). After a number of tries, the attempt is aborted. The interrupted connection can have many causes, including the packet filter on the RouteFinder not allowing the operation of Trace Route.

Trace Route lists the path of the data packets all the way to the desired IP address. The path ends when the destination address has been reached. Should the data packets' path momentarily not be traceable, stars (*) appear to indicate a time-out. After a fixed number of time-outs, the attempt is aborted. This can have various reasons (e.g., a packet filter doesn't allow Trace Route). If it is not possible to locate a name despite activated name resolution, the IP address is shown after several attempts instead.

Host – Specify the **IP address** or the name of the other computer to test this tool.

Start – Click the corresponding **Start** button to start the test.



A Sample Trace Route Log

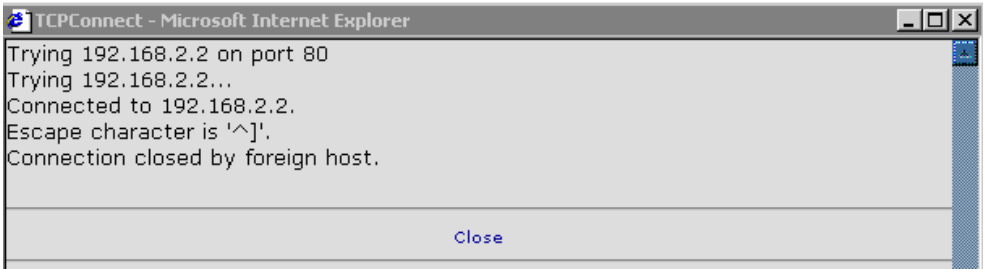
TCP Connect

This tool tests the TCP services for availability. At the IP level, only the source and target addresses are used. TCP, however, additionally requires the use of port numbers. A connection on the TCP level is identified by the source address and port as well as the target address and port.

Host - Enter the IP address or the name of the Host.

Port - Enter the port number into the TCP port entry field. Example: Port number 80 for the HTTP service.

Start - Start the test connection by clicking the **Start** button.

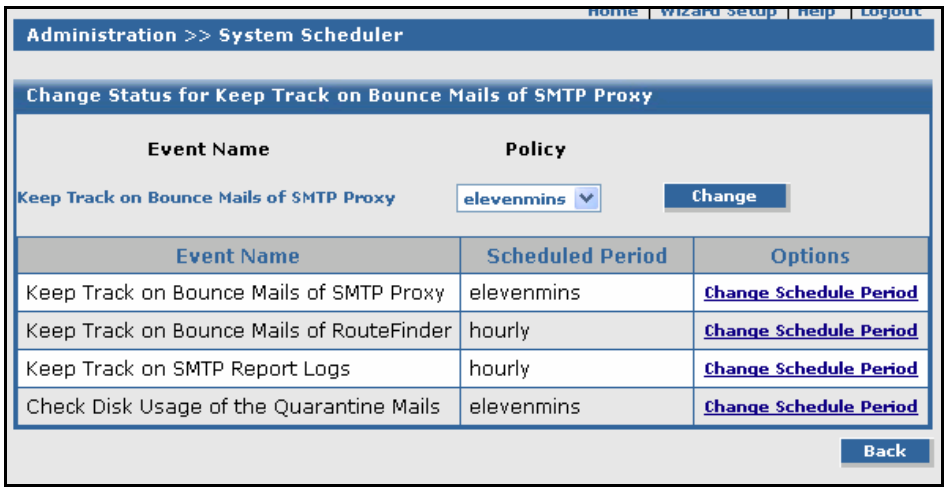


A Sample TCP Connect Log

Administration › System Scheduler

The System Scheduler is a module built into the RouteFinder that ***schedules*** the tracking or checking of the following:

- Tracking bounced emails on the SMTP Proxy
- Tracking bounced RouteFinder emails
- Tracking SMTP Report Logs
- Checking disk usage of quarantined emails

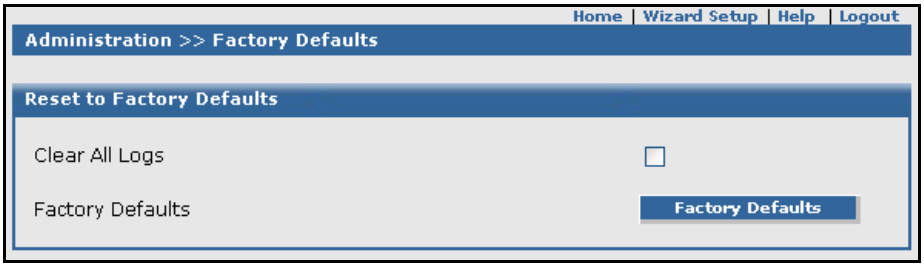


1. Click **Change Schedule Period** for the **Event Name** that you would like to change. Once clicked, the **Event Name** and a drop down list box displays.
2. From the drop down list box, select a new amount of time.
   Each Event offers the following time choices:
   minutely (every minute)
   twomins (every two minutes)
   threemins (every three minutes)
   fivemins (every five minutes)
   sevenmins (every seven minutes)
   elevenmins (every eleven minutes
   thirtymins (every thirty minutes)
   hourly (every hour)
   daily – 1 (once a day)
   daily – 2 (twice a day)
   daily – 3 (three times a day)
   midnight (each day at midnight)
   weekly (once a week)
   fortnightly (once every two weeks)
   monthly (once a month)
3. Click the **Change** button. The new time selection is scheduled and displays in **Scheduled Period**.

Administration › Factory Defaults

Click the **Factory Defaults** button on this screen to return all RouteFinder settings to the original factory defaults. This will change **all** the settings you have modified. You may want to record current settings for referencing later on.

You have the option to Clear All Logs before resetting the factory defaults.



Administration › User Authentication › Local Users

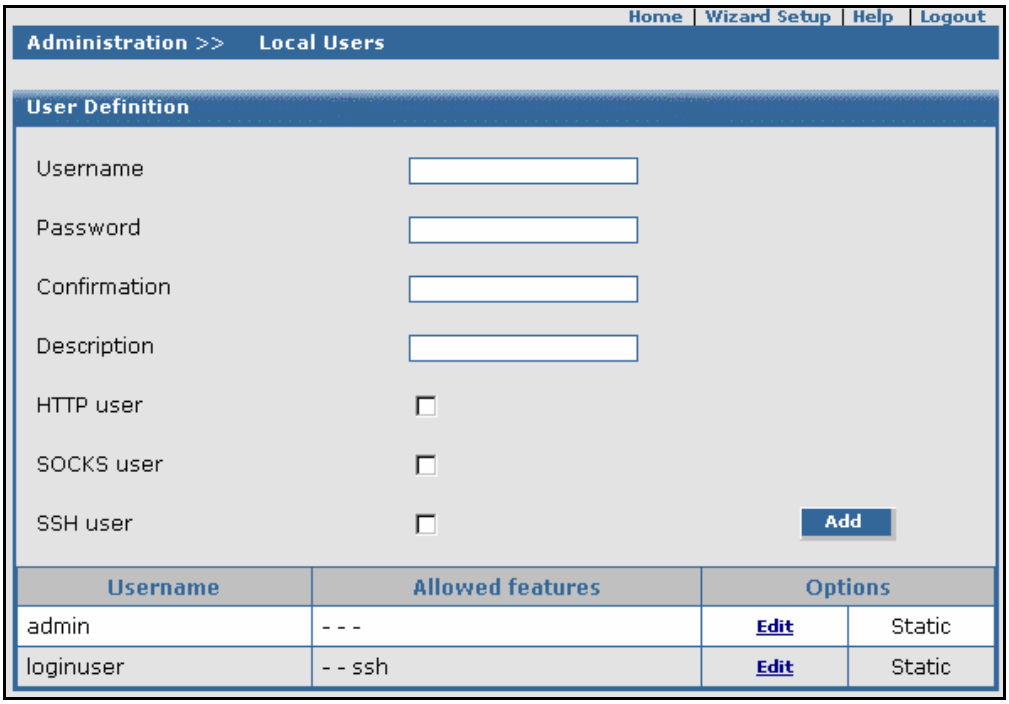
In this part of the software **enter local users** and **define their access to various proxies.**

External user databases can also be accessed (e.g., RADIUS servers, Windows NT servers, or Windows 2000 servers). User Authentication is useful if a user database already exists on such a server, in which case the user need not be created on the RouteFinder again.

At the IP level, you can limit the access to the proxy services of your RouteFinder by setting **Packet Filter rules** on your internal clients. This poses certain problems, however, if you are using a dynamic configuration protocol internally, such as DHCP or BOOTP. In this case, user authentication becomes irrelevant. When requests are made to a proxy service, the client must authenticate himself with his user name and password. This makes the authentication person-based (i.e., user-based) and not IP-based, thus making a person-based Accounting in the HTTP proxy access protocol possible.

Prerequisite

Before you can use Local Authentication, you must activate **User Authentication** for the respective proxy services. In **Proxy** (e.g., **Proxy > HTTP** or **Proxy > SOCKS**) check the **Local** in the Authentication Types menu; then click **Add**.



User Definition

User Name Enter the name of the user. This is a required field.

Password Enter the user's password. The password should be a minimum of 8 characters.

Confirmation Confirm the password entered above by entering it again.

Description Enter a short comment that will identify the user to you.

HTTP User Check this checkbox if you want the user to have access to the HTTP proxy.

SOCKS User Check this checkbox if you want the user to have access to the SOCKS proxy.

SSH User Check this checkbox if you want the user to have SSH access.

Add Button Click **Add** after all the parameters are entered. After a successful definition, the new user displays in the user table.

Edit or Delete You can edit or delete entries in the table by highlighting the desired entries and clicking **Edit** or **Delete** under **Command**.

Administration › User Authentication › RADIUS & SAM

RADIUS (**Remote Authentication Dial-In User Service)** is a protocol with which equipment such as an ISDN router can access information from a central server for user authentication. It also manages technical information needed for the communication of the router with the equipment of the caller. This includes, for example, the protocols used, IP addresses, telephone numbers, timeouts, routes, etc. Together they create a user profile that is stored in a file or a database on the RADIUS server. RADIUS is also used as a generic authentication protocol.

The RADIUS protocol is very flexible and is available for most operating systems, including Microsoft Windows NT/2000. RouteFinder RADIUS implementation lets you configure access rights on the basis of proxies and users.

A RADIUS server should not be visible to the world at large, but should be contained behind the firewall. If the RADIUS server is visible from the Internet, a number of attacks become possible.

Note: In order to use any of these authentication methods, you must activate user authentication and the type of authentication for the services. Mark the option (Local, SAM, RADIUS) in the select menu of the respective services. SSH by default authenticates users using the local system, and you cannot disable local authentication for SSH; whereas, for SOCKS and HTTP, any type of authentication can be enabled or disabled.

RADIUS Prerequisite

Before you can activate **RADIUS** authentication, you need a RADIUS server on your network. The server could also be somewhere in the external network (Internet). But, since the passwords are transferred in plain text, we strongly recommend that the RADIUS server be located close to the RouteFinder and that they are connected via a switching hub. In case of transfer via a public network, we recommend the use of an encrypted tunnel.

RADIUS Settings

RADIUS Server Address

Set the IP address of the RADIUS server.

RADIUS Server Secret

Enter the password for the RADIUS server.

Save

After entering the above parameters, click the **Save** button.

A Note About Microsoft IAS

For information about Microsoft's IAS (RADIUS server for MS Windows NT and 2000), see Multi-Tech's RASExpress RADIUS Setup Reference Guide. The guide also gives you step-by-step setup examples and links to Microsoft's ISA site.

SAM Prerequisite

In order to be able to use this authentication method, your network requires a Microsoft Windows NT or 2000 computer that contains the user information. This can be a Primary Domain Controller (PDC) or an independent server.

This server has a NETBIOS name (the NT/2000 server name) and an IP address.

1. Under the **Administration** menu, open **User Authentication** > **RADUIS & SAM**.

   Domain Enter the name of your MS Windows NT/2000 domain into this field.
   Accepted characters are: the alphabet, the numbers 0 to 9, the minus sign, and underscore.
   Caution: This is not an Internet domain (e.g., *Company.com*) but a simple denominator (e.g., Intranet). If, instead of using the Microsoft domain concept, you only have a simple server, then enter the NetBIOS name. This corresponds to the entry in the PDC name entry field.

   PDC Name Enter the NETBIOS name of the primary domain controller into this field. As of Microsoft Windows 2000, these names are also official DNS names. The RouteFinder only supports names consisting of alphanumeric and minus and full-stop characters. Special characters such as % ! # _ { } are not permitted.

   PDC IP Enter the IP address of the primary domain controller into this field.

   BDC Name If you are using a backup domain controller, enter the name into this field. If you do not have a backup domain controller, enter the PDC name again.

   BDC IP Enter the IP address of the backup domain controller into this field. If you do not have a backup domain controller, enter the PDC IP address again.

2. Confirm your entries by clicking the **Save** button.

Important Note: If you are using SAM authentication, you should deactivate the guest account of your Windows domain. Otherwise all user/password combinations are counted as valid.

SAM

This authentication method uses an MS Windows NT/2000 domain controller or a standalone server to evaluate the requests. Many businesses are already using MS Windows NT/2000 networks that are based on the MS Windows NT/2000 active directory domain concept.

The advantage of SAM is that it is very easy to configure if there is already a PDC (Primary Domain Controller) or a simple server with a user database running in the network.

The disadvantage is that this model cannot discern between different user groups and proxies. This means that you can grant only **all** users or **none** of the users access to a particular proxy.

SAM Settings

Domain
Enter the domain name of the PDC/DC Domain.

Primary Domain Controller Name
Enter the NETBIOS name of the Domain Controller.

Primary Domain Controller Address
Enter the address of the Domain Controller.

Backup Domain Controller Name
Enter the NETBIOS name of the Backup Domain Controller (if present). If you are not using a backup domain controller, then you can enter Primary Domain Controller name in this field.

Backup Domain Controller Address
Enter the address of the Backup Domain Controller.

Save
After entering the above parameters, click the **Save** button.

Administration › Restart

1. Click the **Restart** button to shut down and restart the RouteFinder.
   The message ***Are you sure you want to restart the system?*** is displayed.
2. Click the **OK** button to confirm that you want to restart the RouteFinder WebAdmin software. The complete restart can take 4 to 5 minutes. When the restart process is complete, the RouteFinder will generate 5 consecutive beeps; you can now continue RouteFinder operation.
   If you do not want to restart the RouteFinder software, click **Cancel**.

Administration › Shutdown

1. Click the **Shutdown** button to shut down the RouteFinder. This is the correct way to shut down the RouteFinder. It ensures that all the services are shut down correctly.
   Are you sure you want to shutdown the system? message displays.
   - If you do not want to shut down the RouteFinder, click the **Cancel** button to return to the **Administration > Shutdown** menu.
   - If you want to shut down the RouteFinder, click the **OK** button to confirm.

The Login screen displays while the shut down process takes place (2 to 5 minutes). A continuous beep occurs when shutdown is complete. At this point you can power off the RouteFinder.

Caution: You should switch off the RouteFinder power only after you have performed this **Shutdown** process. If the RouteFinder is not properly shut down before switching off Power, the next start may take a little longer. In the worst case, data could be lost. Since the RouteFinder is now also checking the consistency of the file system, it may have to restart up to three times.

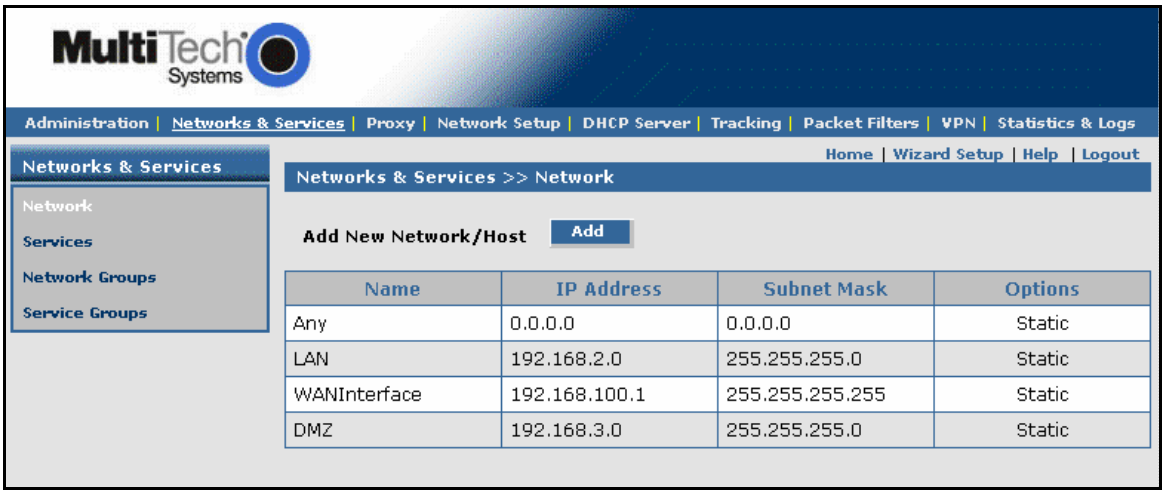
Networks & Services

Networks & Services › Networks

A network always consists of a Name, an IP address, and a Subnet Mask address. Once you add a network, the information displays at the bottom of the screen. This network table contains some generic networks by default, which cannot be deleted or edited.

Important Notes:

- LAN and WAN interfaces will change if changes are made to LAN/WAN IP addresses in Network Setup.
- To define a single host, enter its IP address and use a netmask of 255.255.255.255. Technically, single hosts are treated in the same way as networks.
- You can also use the bit "spelling" for the Subnet mask (e.g., write 30 instead of 255.255.255.252).
- A network or host can be deleted only if it is not used for any route or by any other module.
- If a network is being used by a routing section, that network cannot be edited. Similarly, if a host address is edited and changed to a network address, and if that host was used by SNAT or DNAT, the changed will not be performed.



Add Network

Name

Enter a straightforward name into the Name entry field. This name is later used to set packet filter rules, etc. Accepted characters: alphabetic, numerical 0 to 9, the minus sign, underscore. Maximum characters are 39.

IP Address

Enter the IP address of the network.

Subnet Mask

Enter the Net Mask.

How to Confirm Your Entries

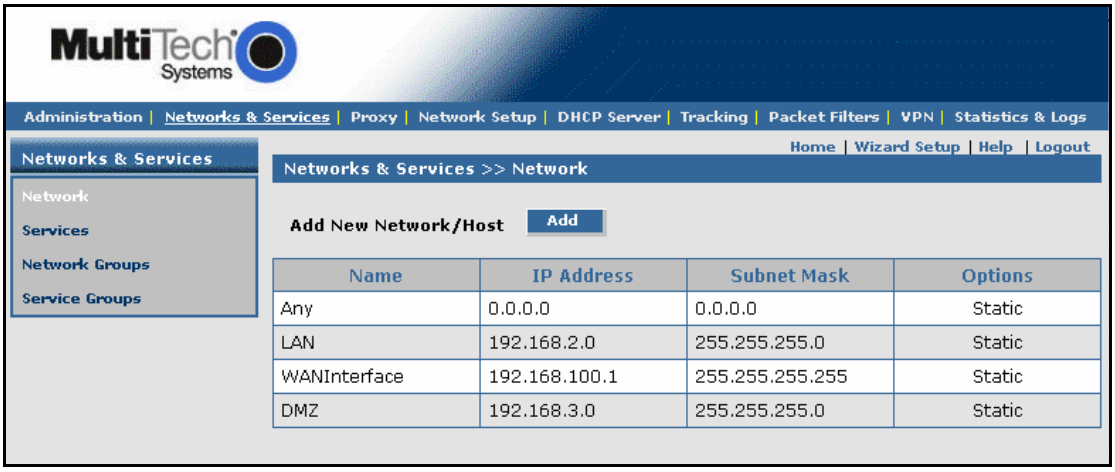
Confirm your entries by clicking the **Add** button.

After a successful definition, the new network is entered into the network table. This network will now be referenced in other menus under this name. You can edit and delete networks by clicking **Edit** or **Delete** in the **Options** column for the network you want to change. The **Edit Network Publications** (in this example) is displayed. The name of the network cannot be changed, but the IP Address and Subnet Mask can be edited. You can delete a newly created network by clicking on **Delete** in the Options column for a desired network.

Example 1: IP address 192.168.2.1 Subnet mask 255.255.255.0 Define a private Class-C net.
Example 2: IP address 216.200.241.66 Subnet mask 255.255.255.255 Define a host in the Internet.

Note About Entries: Entries can be made in the dot notation style (e.g. 255.255.255.0 for a class C network).

After clicking the **Add** button, the Networks you have setup display on the lower part of the screen.



Example 1 – After the networks in the example are added, you will see the following entries added to the table on this screen:

Name	IP Address	Subnet Mask	Options
RemoteLAN	192.168.100	255.255.255.0	Edit | Delete
RemoteWAN_IP	204.26.122.3	255.255.255.255	Edit | Delete

Notes:

- The first four networks on this screen are default entries and cannot be changed.
- Networks added using the **Add Network/Host** function on this screen will also display in the *Remote Gateway IP* and *Remote LAN* dropdown boxes on the **VPN > IPSec > IKE** screen.

Entries on This Screen Affect Other Screens

Networks added on this screen will display on the following screens:
Administration Access Network Groups SSH Packet Filter Rules Network Intrusion Detection Routing Masquerading SNAT DNAT HTTP Proxy SMTP Proxy DNS Proxy IPSec PPTP
Network Names added on this screen will be made available to:
Add Allowed Networks on Administration Access screen *Add packet filter rules* *Add source* for Destination Networks on the Network Intrusion Detection screen *Add Routes* on the Routing screen SNAT Masquerading Port scan detection and DNAT sections *Add allowed networks* on SSH, HTTP Proxy, and DNS Proxy screens *Add relay networks* on SMTP Proxy screen *Add subnets* on IPSec screen *Add local and remote IP addresses* on PPTP screen *Mac address filtering (destination IP address)* on the Packet Filters > Advanced screen

Networks & Services › Services

On this screen you can set the RouteFinder protocol services. Protocols make ongoing administration easier and enable the configuration of user-defined services. These services are used in many of the other configuration settings on the system. A service protocol setting consists of a **Name**, the **Protocol**, the **S-Port/Client** (source port), and the **D-Port/Server** (destination port).

Name	Protocol	S-Port	D-Port	Options
Any	any	1:65535	1:65535	Static
AH	ah	0	0	Static
DNS	tcp/udp	1:65535	53	Static
ESP	esp	0	0	Static
FTP	tcp	1024:65535	20:21	Static
FTP-CONTROL	tcp	1024:65535	21	Static
GRE	gre	0	0	Static
H323	tcp	1024:65535	1720	Static
HTTP	tcp	1024:65535	80	Static
HTTPS	tcp	1024:65535	443	Static
IDENT	tcp	1024:65535	113	Static
IMAP	tcp	1024:65535	143	Static
netbios-dgm	tcp/udp	138	138	Static
netbios-ns	tcp/udp	137	137	Static
netbios-ssn	tcp/udp	1024:65535	139	Static
NEWS	tcp	1024:65535	119	Static
POP3	tcp	1024:65535	110	Static
PPTP	tcp	1024:65535	1723	Static
SMTP	tcp	1024:65535	25	Static
SNMP	udp	1024:65535	161	Static
SNTP	tcp	1024:65535	123	Static
SOCKS	tcp	1024:65535	1080	Static
SQUID	tcp	1024:65535	3128	Static
SSH	tcp	1:65535	22	Static
TELNET	tcp	1024:65535	23	Static
TRACEROUTE	udp	1024:65535	33000:34000	Static

Name	Protocol	ICMP Type	ICMP Code	Options
Name	Protocol	SPI		Options

Add Services

Name Enter a unique name in Name entry field. You will need this later (e.g., to set packet filter rules). The name should not be present in the service or service group list. Using a space in the name is not allowed. After you have entered the name, click the **Add** button.

Protocol Select from the following protocols: **TCP, UDP, TCP & UDP, ICMP, AH, and ESP**. When you select a protocol, the corresponding protocol fields will display.

Source Port Enter the source port for the service. The entry options are a single port (e.g. 80), a list of port numbers separated by commas (e.g. 25, 80, 110), or a port range (e.g. 1024:64000) separated by a colon (**:**). It will be displayed if the type of the protocol is TCP, UDP, or TCP+UDP.

Destination Port Enter the destination port for the protocol. It is displayed if the type of protocol is TCP, UDP, or TCP+UDP.

ICMP Code Specifies the ICMP type. It is displayed if the type of protocol is ICMP and the ICMP Type is *Redirect Network*, *Network Unreachable*, or *Time to Live Exceeded*.

Editing and Deleting User-Added Services

There are options for editing or deleting the user added services. However, there are some standard services which cannot be edited or deleted. If the service is used by the Packet Filter rules, SNAT, or DNAT, it cannot be deleted.

For editing any user-defined service, the **Edit** button has to be clicked to get the fields corresponding to the service entry.

Edit By clicking **Edit** in the Options column, the information is loaded into the entry menu of the **Edit Service** screen. You can then edit the entry. You can edit user-added services only. The entries can be saved using the **Save** button.

Delete By clicking **Delete** in the Options column, the service is deleted from the Services table. Changes can be saved using the **Save** button.

Notes About Protocols

- **TCP & UDP** allow both protocols to be active at the same time.
- The **ICMP** protocol is necessary to test network connections and RouteFinder functionality, as well as for diagnostic purposes. In the **Packet Filter > ICMP** menu you can enable **ICMP Forwarding** between networks, as well as RouteFinder ICMP reception (e.g., to allow **ping** support).
- The **ESP** protocol is required for Virtual Private Network (VPN).
- The **AH** protocol is required for Virtual Private Network (VPN).
- For **AH** and **ESP**, the **SPI** is a whole number between 256 and 65536, which has been mutually agreed upon by the communication partners. Values below 256 are reserved by the Internet Assigned Numbers Authority (IANA).

Entries on This Screen Affect Other Screens

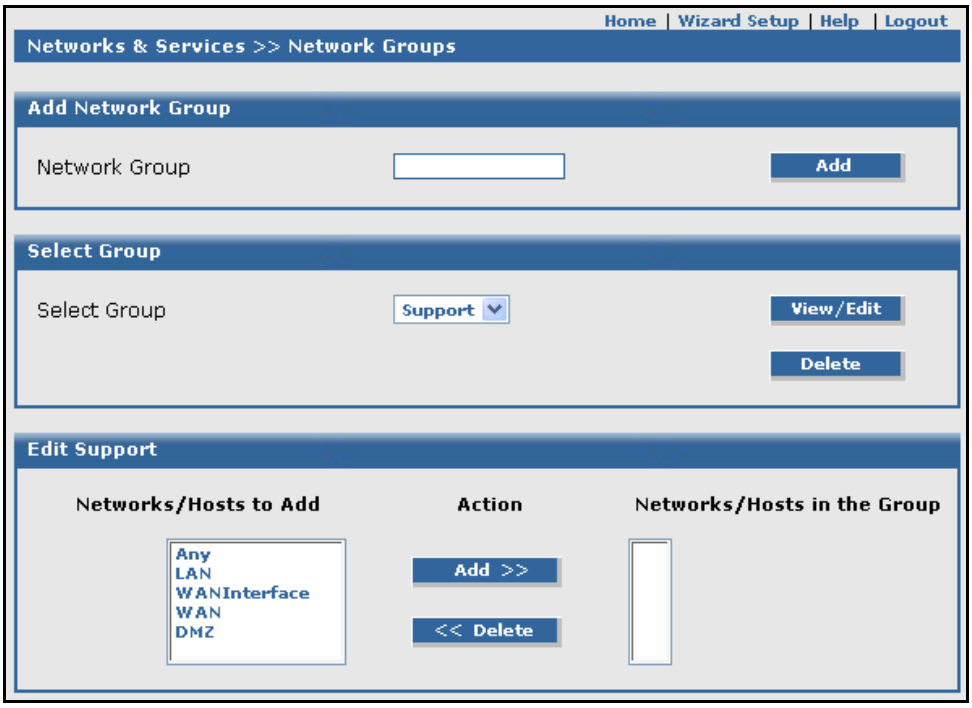
Service Names added on this screen will display on the following screens	
Screen	***Fields***
Packet Filter Rules	*Add packet filter rules*
Packet Filters > Advanced	*MAC Address Based Filtering*
Network Intrusion Detection	*Add specific services for Network Intrusion Detection*
SNAT	*Add rule*
DNAT	*Add rule*

Networks & Services › Network Groups

On this screen you can combine various networks into groups. The networks added in the screen **Network & Services > Networks** can be placed into groups.

Rules and Suggestions for Establishing a Network Group

- A network that is already a part of a group cannot be added to any other group.
- It is suggested that you start a group name with a **G-** or **Group-**. This will identify group network names in contrast to network names.
- When editing Network Groups, note that by pressing the **Shift** key, several entries can be selected together allowing them to be added or deleted together.
- Every change in **Network Groups** is effective immediately.



About the Screen

Initially, the screen opens with only the *Add Network Group* field showing. Once a name is entered, the *Select Group* section displays. When the **View/Edit** button is clicked, the *Edit xxxxxx* section of the screen displays.

Add Network Group

Enter a unique name for the **Network Group**. This name is used later if you want to perform operations such as setting packet filter rules. Click the **Add** button.

Select Group [Group Names Entered Above Now Display Here]

Select the group from the drop-down list box you would like to Edit or Delete.

View/Edit Group

Click the **View/Edit Group** button. This allows you to view and edit the networks which are not part of any group and the list of networks which fall under that group. These networks are available to be part of your newly named network group. The **Edit Support** section of the screen displays.

Delete Group

Click the **Delete** button to delete the group selected.

Edit xxxxx (Networks to Add and Networks in the Group)

Networks to Add

Use the **Networks to Add** button to add networks into the newly named group.

Deleting Networks from a Group

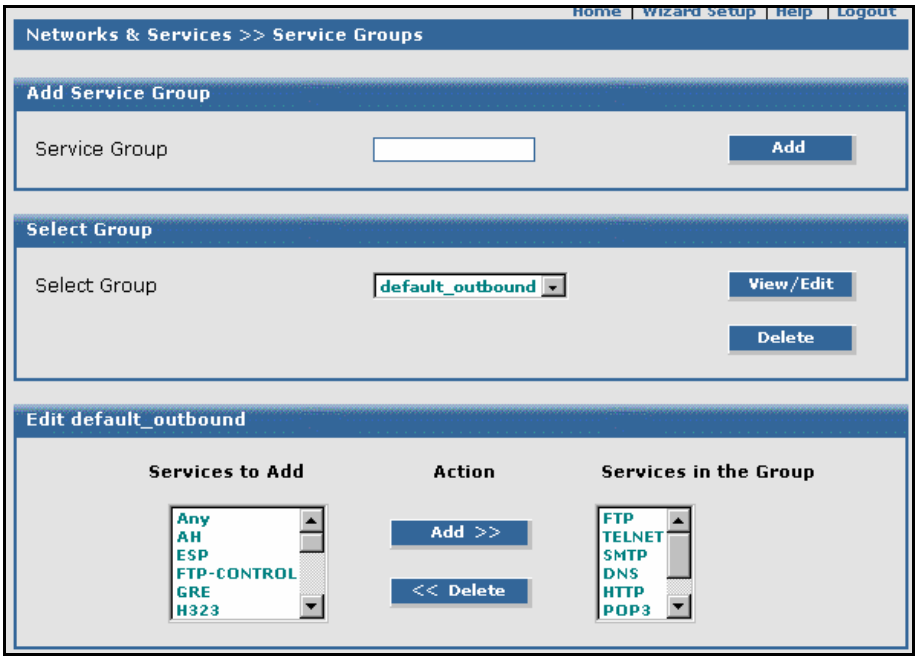
Networks can be deleted from the newly created group by clicking the **Delete Network** button.

Networks & Services › Service Groups

On this screen you can combine multiple Services (see Services section) into groups, called Service Groups. **Service Groups** are treated like single services.

Rules and Suggestions for Establishing Service Groups

- A service that is already a part of a group cannot be added to any other group.
- A service can also be deleted from a group.
- Every change made to **Service Groups** is effective immediately.



About the Screen

Initially, the screen opens with only the *Add Service Group* field showing. Once a name is entered, the *Select Group* section displays. When the **View/Edit** button is clicked, the *Edit xxxx* section of the screen displays.

Add Service Group

Enter a unique name for the **Service Group**. This name is required for later operations such as creating a higher-level service group or to set packet filter rules. Click **Add**.

All names will be added to **Select Group** drop-down list box from which you can **Edit** or **Delete** a Service Group.

Select Group [Group Names Entered Above Now Display Here]

Select the group from the drop-down list box you would like to Edit or Delete.

View/Edit Group

Click the **View/Edit Group** button. This allows you to view and edit the services for that group. The **Edit Support** section of the screen displays.

Delete Group

Click the **Delete** button to delete the group selected.

Edit xxxx (Networks to Add and Networks in the Group)

Services to Add

Use the **Services to Add** button to add services into the newly named group. Available services are:

ANY	H323	IMAP	NEWS	SNMP	SSH
DNS	HTTP	netbios-dgm	PPTP	SNTP	Telnet
FTP	HTTPS	netbios-ns	POP3	SOCKS	TRACE ROUTE
FTP-CONTROL	IDENT	netbios-ssn	SMTP	SQUID	

Deleting Services from a Group

Services can be deleted from the newly created group by clicking the **Delete Service** button.

Proxy

While the packet filter filters the data traffic on a network level, the use of a **Proxy** (also called an Application Gateway) increases the security of the RouteFinder on the application level, as there is no direct connection between client and server.

Every proxy can offer further security for its application protocols. Since each proxy is intended to serve only one or a few application protocols, it usually offers more sophisticated features for logging and real-time analysis of transferred content.

General Information About Proxies

Proxy Services and Authentication Methods

The SOCKSv5 and HTTP proxy services support user authentication. Both proxies can be configured so that they either accept all clients (based on IP addresses), or only those clients with a valid user name and password. If you activate user authentication, you must determine which method your RouteFinder will use to evaluate the requested credentials, otherwise the proxy service cannot be used.

The RouteFinder supports user authentication against:

- RADIUS server
- Windows NT SAM user base
- Defined user database in Administration Access

The three user databases can also be interrogated one after the other.

To Switch Off Proxy Using Netscape Navigator

1. Open the menu **Edit/Settings/Extended/Proxies**.
2. At Manual Proxies Configuration, click the **View** button.
3. At **No Proxy For**, enter the IP address of your RouteFinder.
4. Click the **OK** button to save the entries.

To Switch Off Proxy Using Microsoft Internet Explorer

1. Open the menu ***Extras/Internet*** options.
2. Choose the register card ***Connections***.
3. Open the menu ***LAN Settings/Extended***.
4. Under ***Exceptions***, enter the IP address of your RouteFinder.
5. Click the **OK** button to save your settings.

Rules and Suggestions for Using HTTP Proxy

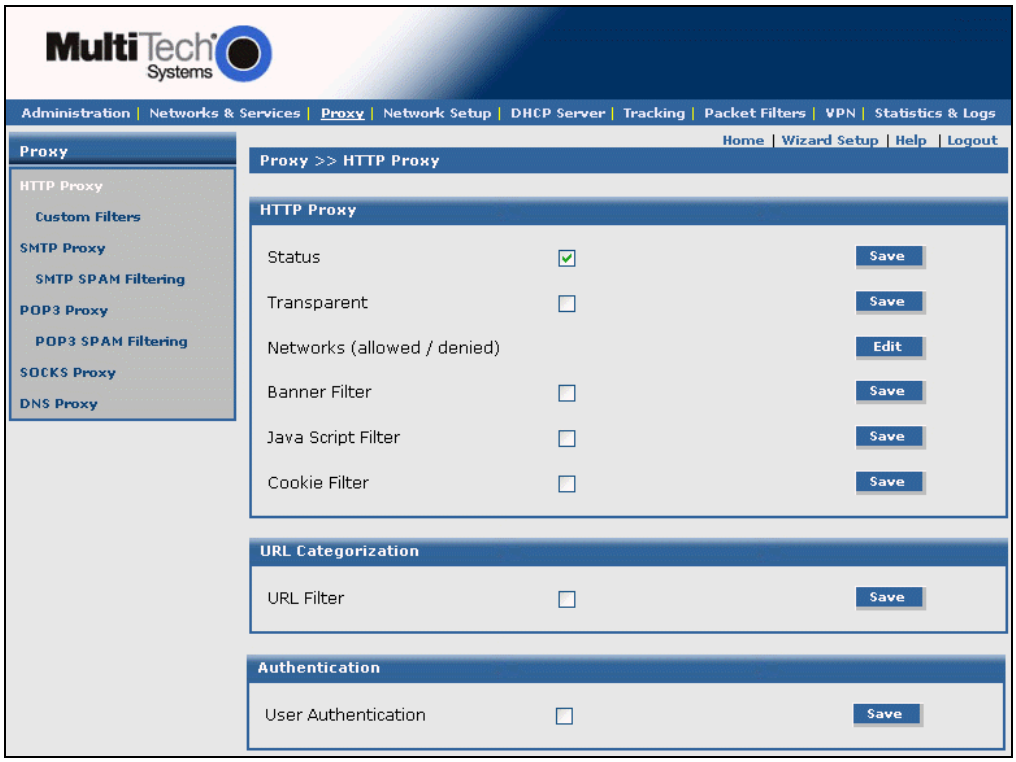
- A valid name server is required for using an HTTP proxy.
- **Administration Access** should not be called up via one of its own proxies. You should configure your Web browser in such a way that the IP address of the RouteFinder is not reached via a proxy.
- The HTTP proxy is an application gateway that converts the HTTP protocol (TCP/IP-port 80) for the transmission of Web pages. To use an active HTTP proxy, you need matching browser settings (TCP/IP address of your RouteFinder and port 3128); otherwise, the proxy must be run in transparent mode. Requests to HTTPS (TCP/IP port 443) are forwarded unchanged.
- Parts of a Web page such as streaming audio and video are not loaded via port 80 (HTTP), but via a different TCP port. These must be dealt with via an appropriate rule in the Packet Filter Rules.

Using Transparent Mode with HTTP Proxy

- While using transparent mode, all networks that should be forwarded transparently to the Proxy must be assigned. All unassigned networks that you want to connect to the Internet without the proxy must be inserted with a corresponding rule in **Packet Filter**. There is no access to the HTTP proxy using predefined settings in the browser in transparent mode.
- If you choose **Non-Transparent mode**, consider the following:
  - You must assign the networks that are to be allowed to use the proxy.
  - No unassigned networks can use the HTTP proxy if the proxy is configured in the browser.
  - You must set up the RouteFinder internal IP and port 3128
  - User Authentication is possible only in non-transparent mode.

Proxy › HTTP Proxy

The HTTP Proxy is capable of transferring **www** requests. HTTP use can be viewed in the **Statistics & Logs** menu.



HTTP Proxy Section

Status

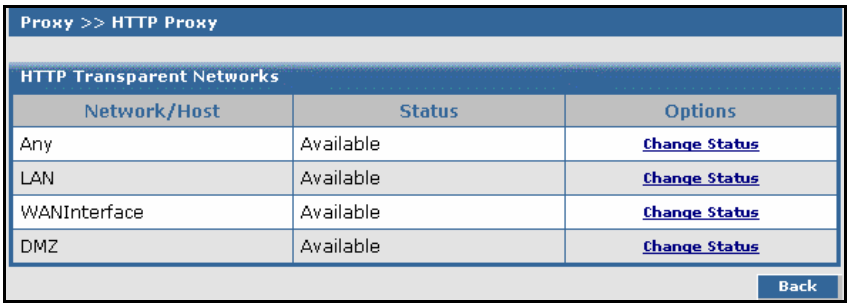
To enable HTTP, check the **Status** box and click **Save**.

Transparent

To enable Transparent mode, place a check mark in the **Transparent** box and click the **Save** button. This mode matches for HTTP requests only via port 80 from the internal network and forwards them to the proxy. This process is invisible to the user. No further administration is required because no changes to the browser setting of the end user are necessary. See the previous page for notes about using Transparent mode.

Networks (Allowed or Denied)

To select the networks you want to be available for the HTTP proxy, click the **Edit** button. The HTTP Transparent Networks screen displays. By clicking the desired Change Status button, you change that network's status to *Allowed, Denied*, as well as *Available*.



Banner Filter, Java Script Filter, and Cookie Filter

To enable any one or any combination of these filters, check the box. Click the corresponding **Save** button each time you enable a filter.

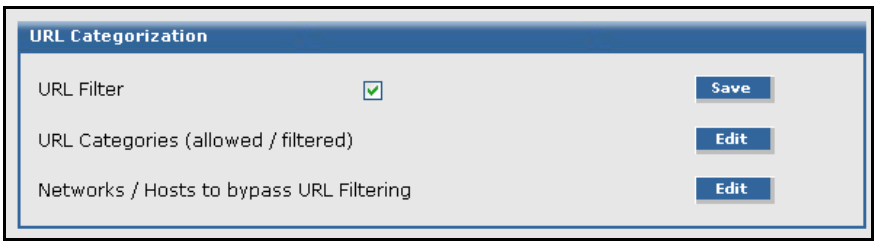
Banner Filter – If this is enabled, then the Web page banners will be filtered out before the page is forwarded to the Web client.

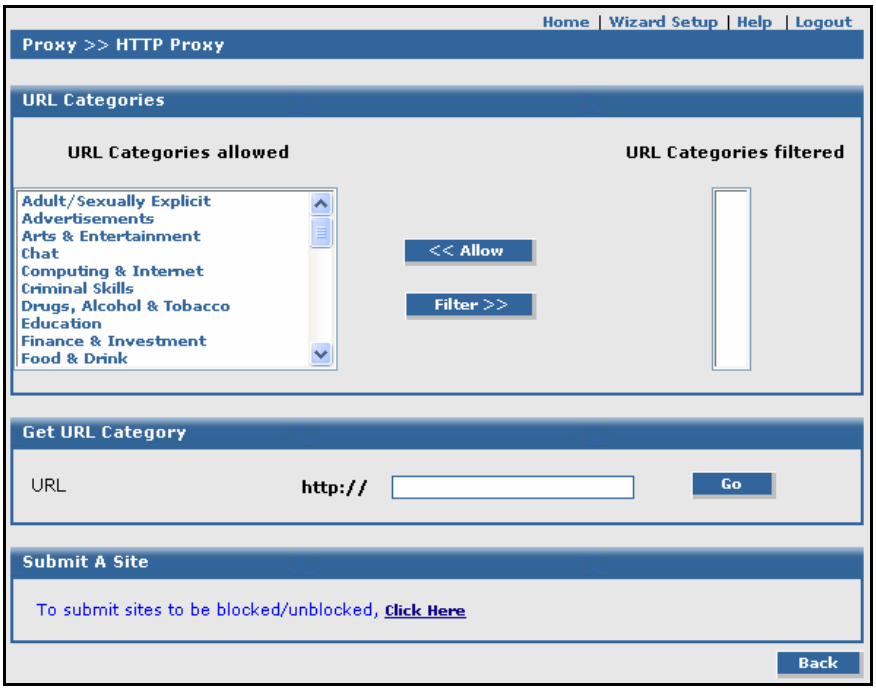
Java Script Filter – If this is enabled, then all the Java Script components in the Web pages will be filtered out before the page is forwarded to the Web client.

Cookie Filter – When this is enabled, then cookies in the Web pages will be filtered out before the page is forwarded to the Web client.

URL Categorization Section of the Main Proxy HTTP Screen

1. Enable URL Categorization by checking the **URL Filter** box on the main Proxy HTTP screen. The URL Categorization section expands as shown here (a cutout section of the main screen with the URL Categorization section expanded is shown here).
2. Click the URL Categories (allowed/filtered) **Edit** button. The URL Categories screens displays. URL Categories can be configured to be filtered/forwarded by the firewall.





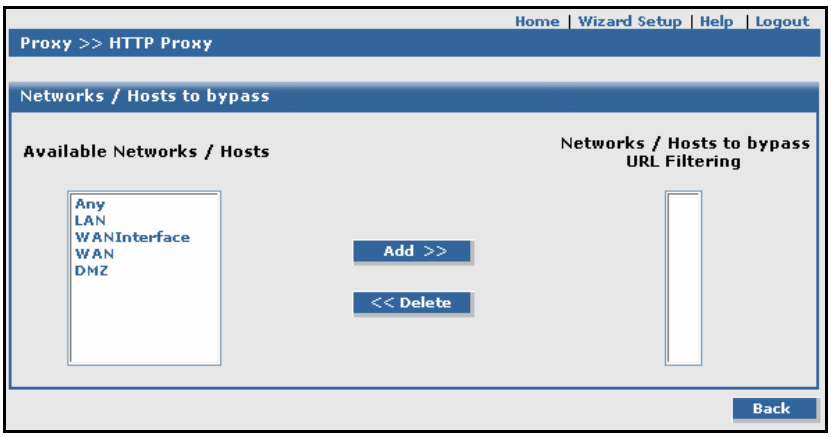
URL Categories (allowed/filtered)

On this screen you can change URL categories from **Allowed** to **Filtered** and *vice versa*). The **Allow** and **Filter** buttons will move a URL Category from **Allowed** to **Filtered** box and back again.

The categories are setup and controlled by SurfControl software, which is built into your RouteFinder. See URL Categorization in Chapter 2 for a detailed discussion of this screen.

3. ***Networks / Hosts to bypass URL Filtering***

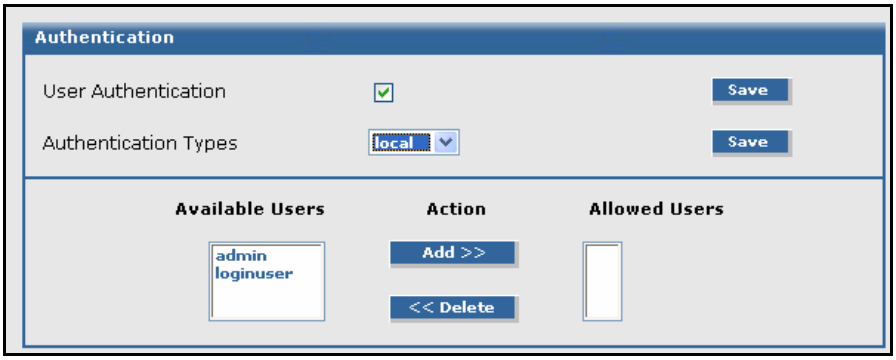
Click the **Edit** button for **Networks / Hosts to bypass URL Filtering**. Use the **Add** button to move a network/host name into the **Bypass URL Filtering** box. If you decide that you do not want one or more of the networks/hosts bypassing the filter, select the name and click the **Delete** button. The name moves back into the Available list.



User Authentication Section of the Main Proxy HTTP Screen

To enable User Authentication, check the **User Authentication** box and click **Save** (a cutout section of the main screen with the User Authentication section expanded is shown here).

Note: If User Authentication is disabled, then the HTTP Proxy can be configured to function in transparent mode.



Authentication Types

1. Select the desired Authentication Type from the drop down list box.
   Available Authentication Types are:
   - Local
   - RADIUS
   - SAM
2. Click the **Save** button.

Available Users

1. Select the User you want to have access to HTTP Proxy server from the **Available Users** list.
2. Click the **Add** button. The user now displays in the **Allowed Users** box.
   You can remove an allowed user by highlighting the name and clicking the **Delete** button. The name goes back to the **Available Users** list.

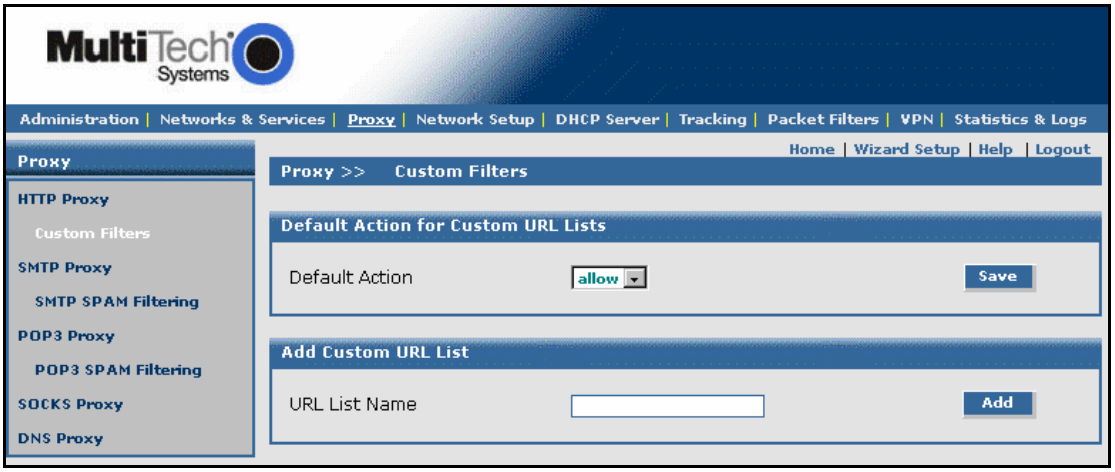
Notes:

Adding New Users: New users can be added to the **Available Users** list on the **Administration > User Authentication** screen.

Non-Transparent Mode: If the HTTP proxy functions in a non-transparent mode, then the authentication mechanism through which the user can be authentication can be configured.

Proxy › HTTP Proxy › Custom Filters

The URL Categories in the HTTP Proxy page allows URLs to be filtered or forwarded by the firewall. On this screen, you can configure Custom Filters. Custom filters will take preference over URL categories. You can use custom filters to build groups of filters or lists that can be filtered by networks. The set of rules for the forwarding and filtered of URLs for a particular network can be configured here.



Default Action for Custom URL Lists

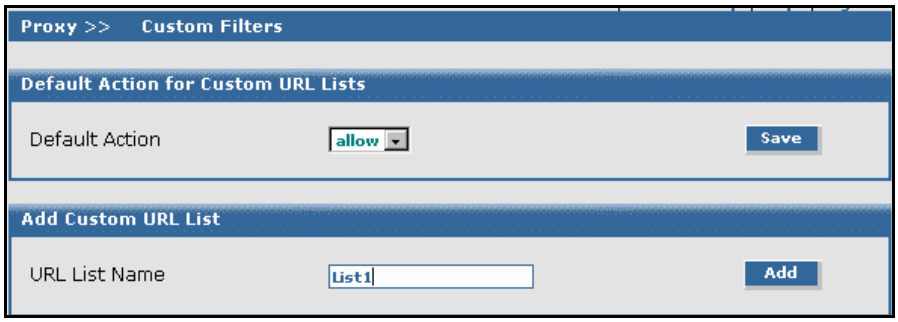
Default Action

Select either **Allow** or **Deny** for your Custom Filter. Click the **Save** button.

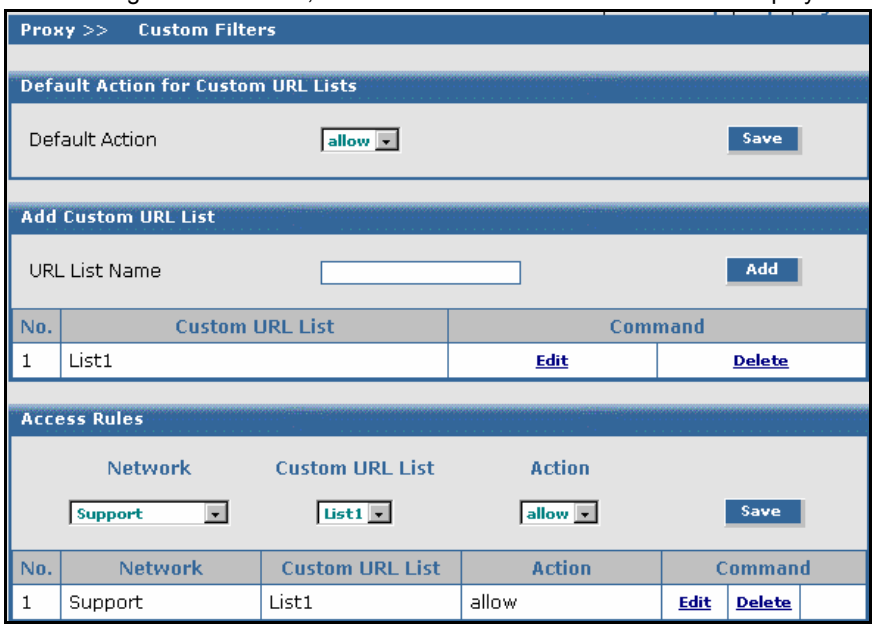
Add Custom URL List

URL List Name

A Custom URL Group or List has to be named before defining a rule. Enter a name for the URL to include in the list here. Click the **Add** button to save the name. On this screen *List1* has been added as a URL group.



After clicking the **Add** button, the *Access Rules* section of the screen displays.



Access Rules

The **Access Rules** function enables you to define custom rules. With these custom rules, networks or network groups can be allowed or denied access to certain URLs. URLs can be added or deleted from this list. Click the **Edit** button to open a screen for entering URLs into the list. A text box and a list box for the URL will be shown. The list box will contain the list of URLs that are already part of this list. URLs can be added to the list by entering it into the text box and clicking the **Add** button.

URLs can be deleted from the list by selecting it and clicking the **Delete** button. Then click the **Save** button.

After making any changes, click the **Save** button to save these changes.

An access rule consists of three parts:

1. Network or Network Group
2. URL Group or List
3. Set either Allow or Deny

Example Using a Group Name

List Name: URL List named ***List1*** contains google.com
Networks: There are two networks ***Net1*** and ***Net2***
Rules: Two rules have been configured:

Net1 – List1 – allow and
Net2 – List1 – deny

What Does This Mean:

- Users from **Net1** trying to access google.com will be allowed to access the site.
- Users from **Net2** trying to access google.com will not be allowed to access the site.
- Users from any other network will be allowed/denied access based on the URL Categorization rules.

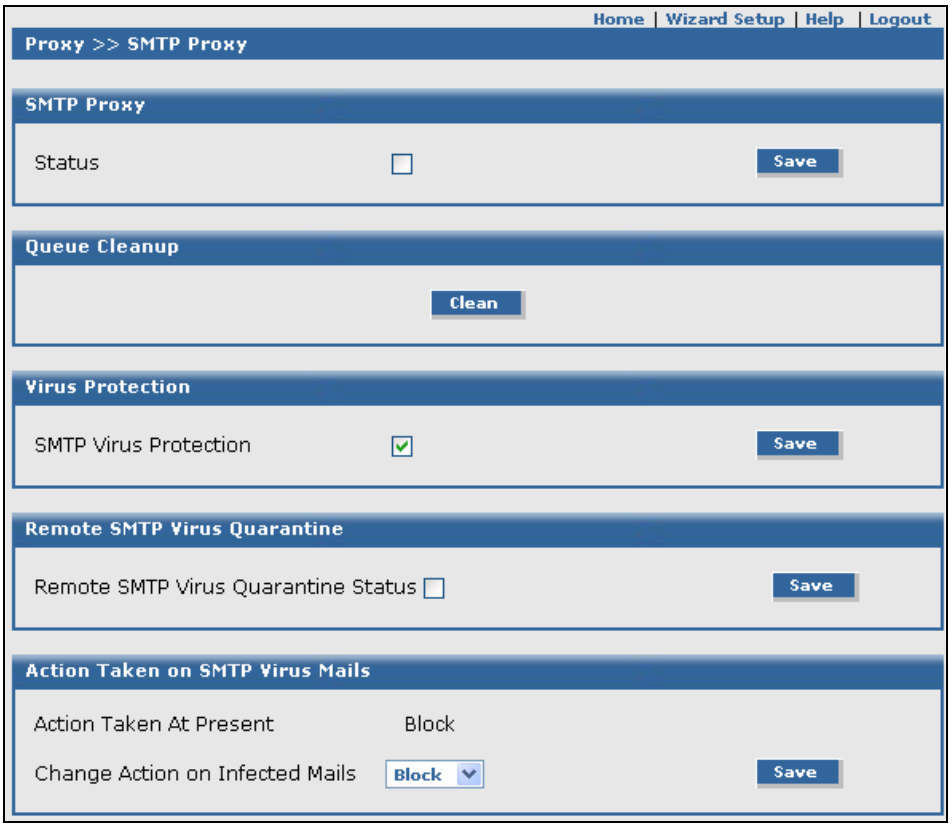
Proxy › SMTP Proxy

On this screen (the full screen displays once the *Status* box is checked), you can configure the SMTP proxy and the Virus Protection function. The SMTP proxy acts as an email relay. It accepts email for your Internet domains and passes them on to your internal email distribution system. This can be accomplished via a Microsoft Exchange Server, for example. Emails are transparently scanned for known viruses and other harmful content.

The SMTP proxy also acts as a gateway for outgoing mail, thus taking over the job of email distribution from your internal email system.

Rules and Suggestions for Using SMTP Proxy

- For **SMTP**, a valid name server (**DNS**) must be enabled. The RouteFinder sends notifications to the administrator even if **SMTP** is disabled. The RouteFinder processes up to 25 incoming SMTP connections simultaneously preventing Denial of Service (DoS) attacks. The 26th incoming connection is not accepted.

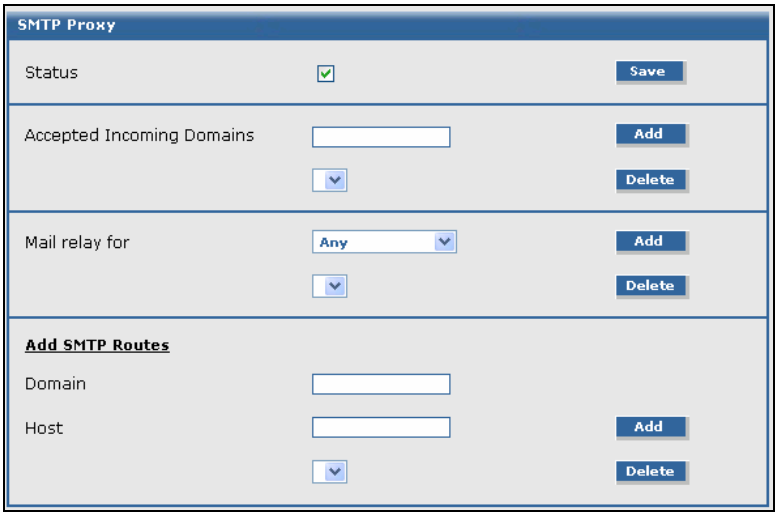


SMTP Proxy

Status

To enable SMTP, check the **Status** box and click the **Save** button. When enabled, the SMTP Proxy starts functioning and listens on port 25.

When **Status** is checked, the screen expands to display the following fields:



Accepted Incoming Domains

All the domains for which the SMTP Proxy can accept emails must be listed here. The domain for which emails are accepted must be registered with the DNS server. Thus, the SMTP Proxy accepts only emails which are addressed to the domains listed here.

Domains will be listed in the drop-down box from which they can be deleted, if desired.

Mail Relay

All the networks that can use the SMTP Proxy as a relay agent are configured here. A list of the various networks configured using this software is displayed. You can add networks that can use the SMTP proxy as a relay agent by using the **Add** button. All other networks not included in this list can send emails to only those domains in the Accepted Incoming Domains list. The IP address of the mail server needs to be added in the list of relay networks.

Add SMTP Routes

The SMTP Proxy decides on the path or the route to be taken for any **domains** based on the SMTP Routes configuration. Thus, the domain name and the IP address of the MTA (Mail Transfer Agent) to which mails are destined to this domain are to be forwarded are listed here.

Example: xyz.com:192.168.1.34. Any email to domain xyz.com is forwarded to 192.168.1.34, which is the IP address of an MTA. If the SMTP route is not mentioned for a domain, then a DNS-lookup decides where this email is to be forwarded or else a default route can be specified so that email to any domain is forwarded to the default gateway. **Example**: 192.168.1.10.

Domain and Host

The fully qualified Domain Name and Host of the SMTP Proxy must be entered here.

Main SMTP Screen Continued

Queue Cleanup

Click the **Clean** button to delete emails held in the relay agent's mail queue. All mails waiting to be delivered will be cleaned up. This option is to be used with extreme care.

Virus Protection – SMTP Virus Protection

Enables/disables virus scanning for SMTP traffic that passes through the RouteFinder. Both incoming and outgoing emails are scanned, if they are sent via the SMTP proxy. If a valid virus license scanner license key is not entered, this option will not be displayed.

An anti-virus license must be purchased from Multi-Tech in order to use virus protection, and the license can be uploaded to the RouteFinder from the **Administration > License Keys** screen.

Remote SMTP Virus Quarantine – Remote SMTP Virus Quarantine Status

Check the ***Remote SMTP Virus Quarantine Status*** box to activate the remote quarantining of SMTP virus emails. If activated, then local quarantining no longer exists.

Action Taken on Virus Emails

Change Action on Infected Mails: Select the action to be taken on infected emails for SMTP traffic.

If the action selected is **Notify**, options to send the information to the administrator / sender / recipient will be displayed. Notification regarding infected mails will be send based on these settings.

If the action is **Block**, the mail will be silently dropped.

In both cases, the infected emails will be stored in the virus quarantine folder of the RouteFinder. The administrator can view the emails, delete them, or forward them to a specified email ID.

Click the **Save** button after a Change Action.

SMTP Proxy Example

An entry *Company.com* covers all further sub-domains; for example, *subsidiary1.Company.com* and *subsidiary2.Company.com*. The RouteFinder must be the MX (Mail Exchanger) for *Company.com*. Incoming emails to non-registered domains are rejected (except for senders listed in Mail relay for below). Confirm every registered domain by clicking the **Add** button. The domains are entered into a window from which the entered domains can be deleted again at any time.

Mail relay for

Select all the networks from the select menu that are allowed to use the **SMTP** proxy on the RouteFinder. Networks not entered here can only use the **SMTP** proxy to send emails to the above listed domains. Confirm every selected network by clicking the **Add** button.

Note: If you assign **Any,** then everybody connected to the Internet can use your SMTP proxy for SPAM purposes.

SMTP Routes

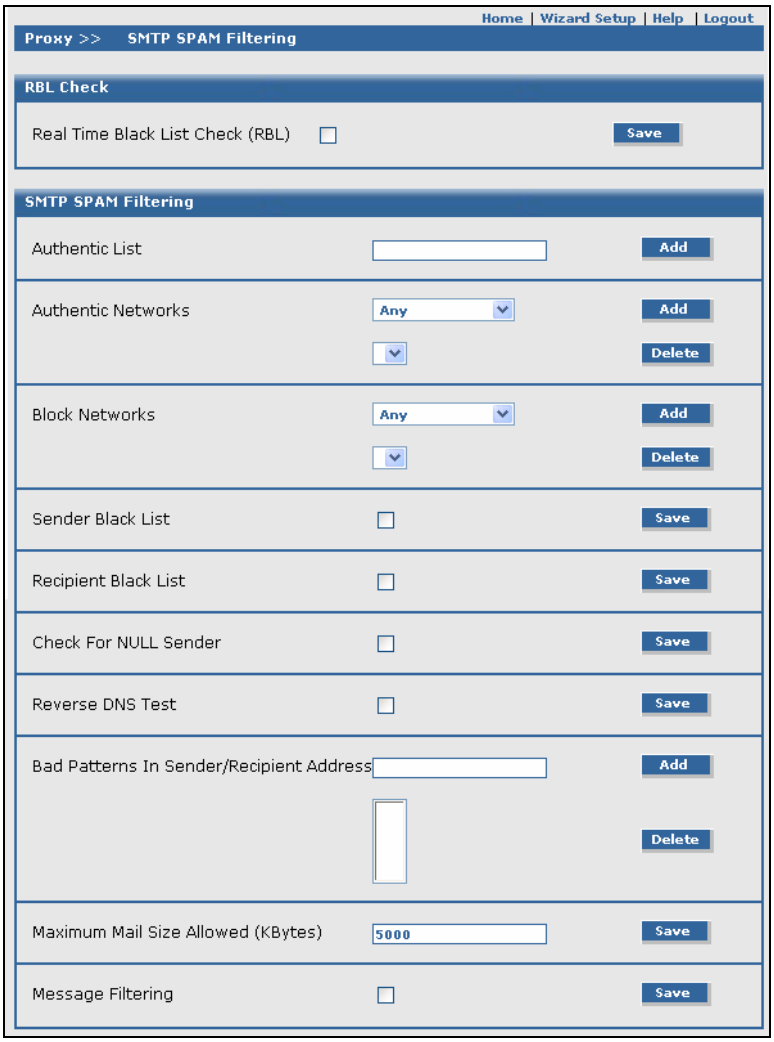
Determine the MTA (Mail Transfer Agent) to which each incoming domain is forwarded. The MTA is determined by its IP address. You can also configure the forwarding of email into your internal messaging system here. If you want to use the SMTP proxy as the SMTP relay (also often called "SmartHost“) for your internal email server, configure it to use the internal address of your RouteFinder system as a relay. However, for this to work, the IP address of your internal email server must have been entered in the Mail relay for select menu. (Remember to insert the forwarding of the domains to your internal email server.)

All outgoing mail is then forwarded via the **SMTP** proxy of the RouteFinder.

All settings are immediately active and are preserved after leaving the **Proxies > SMTP** menu.

Proxy > SMTP Proxy > SMTP SPAM Filtering

On this screen the SPAM filtering parameters can be set so that all incoming and outgoing emails sent to the internal mail server(s) will go through the SPAM filtering process.



RBL (Real Time Black List) Check

Real Time Black List (RBL) – Check this box to block emails from the IP addresses listed in RBL sites. If emails are to be blocked, the IP address or URL of an RBL server must be entered. If you check RBL, then you will be provided with the list ***Authentic List***. Here you can configure IP addresses for which the RBL check can be bypassed.

RBL Server URL – Enter the IP address of the sites to be blocked. Then click **Save**.

Spam Filtering

Authentic List – Enter any sender's email ID that you wish to bypass the spam filtering process.

Authentic Networks – Enter any sender's network name that you wish to bypass the spam filtering process.

Example: *testuser@routefinder.yourdomain.com*

If you want to add email IDs from the domain r*outerfinder.yourdomain.com*, then add it as:
@routefinder.yourdomain.com

Blocked Networks – Enter the name(s) of any network(s) from which email cannot be sent. If any user tries to send an email from a blocked network, the email connection is rejected.

Sender Black List – Enter a sender email addresses to be blocked. Then, if the sender's email address matches any entry in the list, the email will not be forwarded.

If all emails from a domain are to be blocked, add this @ symbol before the domain name:
testuser@routefinder.yourdomain.com

If you want to block all email from the domain *routefinder. yourdomain.com*, then add it as
@routefinder.yourdomain.com

If you want to block all email from the domain *routefinder. yourdomain.com*, then add it as
@routefinder.yourdomain.com

Recipient Black List

Enter a recipient's email address to be blocked. Then, if the recipient's email address matches any entry in the list, the email will not be forwarded.

If all email from a domain is to be blocked, add this @ symbol before the domain name:
testuser@routefinder.yourdomain.com

If you want to block all email from the domain *routefinder. yourdomain.com*, then add it as
@routefinder.yourdomain.com

Check for NULL Sender

If you check this option, email with an empty sender address sent to more than one recipient will not be relayed.

Note: If the email contains only one recipient ID, even if this option is checked, the email will be relayed to the recipient, since it is legitimate to have NULL sender address in error.

Reverse DNS Test

If you check this option, the SMTP Proxy will try to resolve the domain name part of a sender's email ID. If it is resolved to an IP address, then the email will be relayed. If the sender's name is in the Authentic List, then the reverse DNS test will not be performed for the domain.

Bad Patterns in Sender/Recipient Address

Enter any pattern in an email address that you would like to block. Then both the sender and recipient email addresses will be checked for these patterns. If the patterns match, the email will not be relayed.

Control Characters:

1. Exclamation mark (!): Bypass the SPAM check for this entry alone.
   Example: All email from or to the domain *abc.com* will be stopped except for *test@abc.com*:
   *@abc.com
   !test@abc.com
2. Asterisk (*): Stop all email from or to this domain.
   Example: All email from or to the domain *abc.com* will be stopped.
   *@abc.com
3. Set ([…]): Stop all email from a set such as *@abc[0-9]*.com*.
   Example: All email from or to the domains that include numbers in the first part of their names such as *0, 234,* or *789023* will be stopped.
   0.com
   234.com
   789023.com
4. Question mark (?): Stop all email with a match zero or one occurrence of the preceding character or set of characters.
   Example: All email from or to the domains *abc.com*, *abc0.com*, *abc1.com*, …*abc9.com.*
   *abc[0-9]?.com
5. Backslash (\): Literal expression of the following character (the following character is a metacharacter):
   @\[[0-9]{1-3}\[0-9]{1-3}\[0-9]{1-3}\]
   The first two characters after the @ character \[means take the literal value of the [character.
   Example: All email addresses with IP addresses like *username@[1.1.1.1]* will not be allowed.

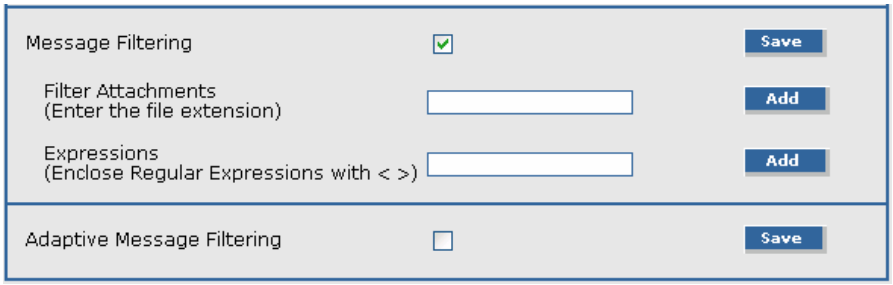
   Note: SPAM emails with percent-hack can be eliminated by adding *%* to the **Bad Patterns** list.

Maximum Mail Size Allowed

The size of each email will be compared with the Maximum Size entered here, and if the mail size is more than the Maximum Size, then that mail will not be relayed. This check will be bypassed for users added to the **SPAM Filtering Authentic List** (on this same screen).

Message Filtering

When **Message Filtering** is checked, the screen expands to display the following fields:



Message Filtering. If you check this option, then the email message or body will be searched for the extensions and expressions added here. If there is a match, the email will be quarantined so that the administrator can decide whether to forward or delete the email.

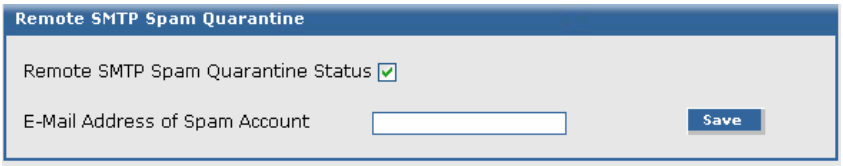
Note About Extensions: Examples of extensions are bmp, exe, gif. Also, double extensions such as tar.gz cannot be used.

Note About Expression Format: If you want to search for the expression *as is* in the email, then add it just as it is. If you want to use the entry as a regular expression, then enclose the entry with these brackets: < >

Note About Wild Card: The wild card '*' cannot be used to filter all attachments.

Adaptive Message Filtering.
If this operation is enabled, then the mail message or body will be searched for auto-learned expressions by the Adaptive Message Filtering function. Click the **Help** button for this screen to read more about Adaptive Message Filtering.

Remote SMTP SPAM Quarantine. This screen displays when **Message Filtering** is checked.



Check the **Status** box to enable Remote SMTP SPAM Quarantining, which will send all SMTP SPAM emails to the configured email address entered into the **E-Mail Address of Spam Account** field.

Click the **Save** button.

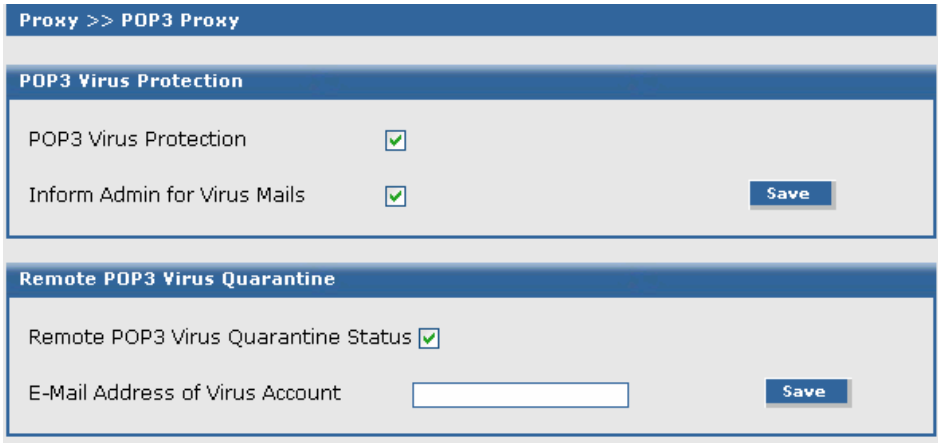
Note: If remote quarantine is enabled, then local quarantine no longer exists.

Proxy › POP3 Proxy

In order to use this function, you must have a valid Antivirus Scanner license key installed. To install one, go to the *Administration* > *License* > *Virus Scanner* page.

Use this screen to configure POP3 virus filtering-related settings. All outgoing email will go through this POP3 virus filtering process.

Note About This Screen: Initially, only the **POP3 Virus Protection** prompt and the **Remote POP3 Virus Quarantine Status** prompts display. The other two prompts display after checking the initial check boxes and clicking the **Save** button.



POP3 Virus Protection

POP3 Virus Protection – Check the box to enable POP3 virus scanning of the traffic that goes through the RouteFinder. Click the **Save** button.

Inform Admin for Virus Mails – Check this box to have information sent to the administrator. The administrator will receive notification regarding infected emails.

Save – Click the **Save** button to activate this function.

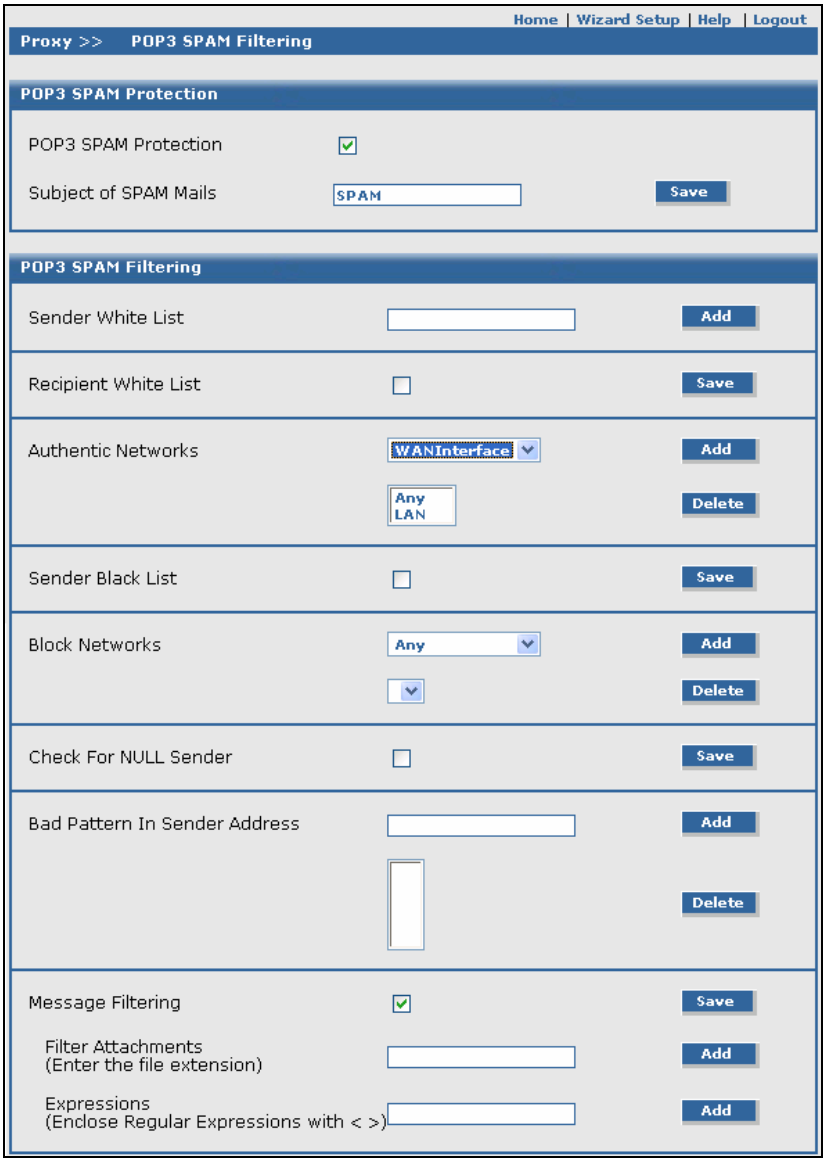
Remote POP3 Virus Protection

Remote POP3 Virus Quarantine – Check the **Status** box to enable POP3 virus scanning of the traffic that goes through the RouteFinder. Click the **Save** button.

Email Address of Virus Account – Enter the address of the POP3 Virus Email Account. All POP3 virus quarantined emails will be forwarded to this account. Click the **Save** button.

Proxy › POP3 Proxy › POP3 SPAM Filtering

The administrator can configure POP3 SPAM filtering and related settings on this screen. All outgoing email retrieved from the internal mail server(s) will go through this POP3 virus filtering.



POP3 SPAM Protection

POP3 SPAM Protection

Check the box to enable POP3 SPAM Protection.

Subject of SPAM Mails

Enter a word that you would like to add to the subject line of any email identified by the virus scanner as SPAM. The word *SPAM* is a good choice.

POP3 SPAM Filtering

Sender White List

Enter the sender email IDs that will **not** be checked for SPAM. For example, if all the emails from the specific domain abc.com are not to be checked for SPAM, then the entry should be @abc.com.

Once you enter the ID and click the **Add** button, the ID displays in a list below the entry field. You may enter more than one email ID, and each ID can be deleted.

Recipient White List

Enter the recipient email IDs that will **not** be checked for SPAM. For example, if all the emails from the specific domain cde.com are not to be checked for SPAM, then the entry should be @cde.com.

Once you enter the ID and click the **Add** button, the ID displays in a list below the entry field. You may enter more than one email ID, and each ID can be deleted.

Authentic Networks

Select the network from which a user may retrieve unfiltered email. In other words, the email on this network is not checked for SPAM. Select from *Any, LAN, WANInterface, DMZ.*

Once you select a network and click **Add**, the network displays in a box below this entry field. You may select more than one network, and a network can be deleted whenever you want to make a change.

Blocked Networks

If the user tries to retrieve email from the network entered in the list, then that connection of retrieving emails is rejected.

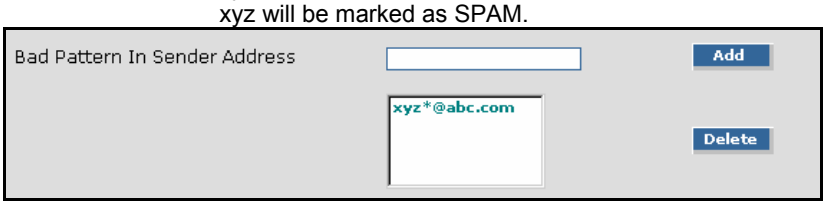
Check for NULL Sender

If this option is enabled, email with an empty sender address is marked as SPAM.

Bad Pattern in Sender Address

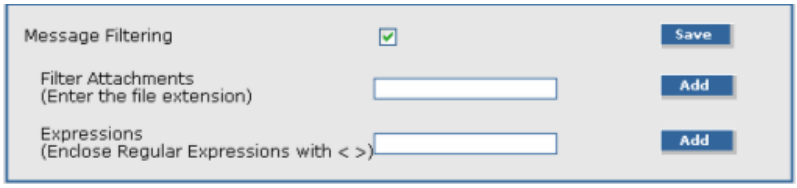
The sender email address will be checked to see if matches any of the patterns added the list. If there is a match, then the email will be marked as SPAM.

Control Character: Asterisk (*) is a general pattern-matching character. For example, if the entry is xyz*@ abc.com, then all email from the domain abc.com with user names starting with xyz will be marked as SPAM.



Message Filtering

If you check Message Filtering, two additional prompts display. File attachments and specified expressions will be filtered.



Attachment Filtering

Enter the file extensions to be filtered. Email will be searched for these extensions. If there is a match, the email will be quarantined so that the administrator can decide whether to forward or delete the email.

Note About Extensions: Examples of extensions are bmp, exe, gif. Also, double extensions such as tar.gz cannot be used. The wild card '*' cannot be used to filter all attachments.

Expression

The email message and body will be searched for the expressions added here. If the expression is "as is" is to be searched for in the email, it is added with quotation marks. If the entry is to be used as a regular expression, the entry should be enclosed in < >.

Proxy › SOCKS Proxy

SOCKS is a universal proxy supported by many client applications. SOCKS5 is an IETF (Internet Engineering Task Force) approved standard, proxy protocol for TCP/IP-based networking applications. The basic purpose of the protocol is to enable hosts on one side of a SOCKS server to gain access to hosts on the other side of a SOCKS Server without requiring direct IP access. When an application client needs to connect to an application server, the client connects to a SOCKS proxy server. The proxy server connects to the application server on behalf of the client and then relays data between client and the application server. For the application server, the proxy server is the client.

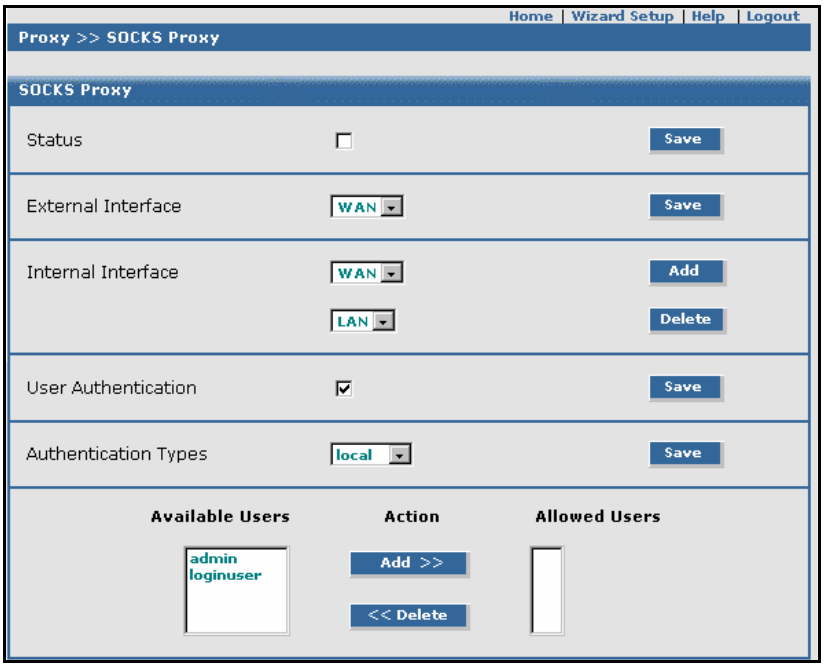
Differences Between SOCKS and NAT:

- SOCKS allows BIND requests (listening on a port on behalf of a client; however, very few clients support this function)
- SOCKS5 allows user authentication.
- The SOCKS proxy is used for point-to-point connections.

The RouteFinder's SOCKS implementation supports the SOCKS v4 and the SOCKS v5 protocol versions. However, when using SOCKS v4, **User Authentication** is not possible.

Socks Default Port – 1080. Almost all clients will default to this port setting, so it normally does not need to be configured.

Notes: All changes in **Proxy** become effective immediately without additional notice.



SOCKS Proxy

Status

To enable SOCKS, check the **Status** box. Click the **Save** button.

External Interface

The SOCKS Proxy uses an external interface to send outgoing requests. Select the interface that you want to use. The options are LAN, WAN, and DMZ. This is the external interface to the Internet.

Internal Interface

Select one or two interfaces on which SOCKS is to accept connections from clients. The options are LAN, WAN, and DMZ. The interfaces listed here can be used by clients with port 1080 to access the SOCKS proxy.

User Authentication

To enable User Authentication, check the User Authentication box. If this function is enabled, SOCKS proxy users must log in with their user names and passwords. User Authentication is available with SOCKSv5 only. If you are using SOCKSv4, User Authentication is not available.

Authentication Types

Select the method of user authentication. Options are Local, RADIUS, and Sam. If you choose the Local method, you can choose whether or not local users may use the SOCKS proxy.

If you disable User Authentication, then client applications must be configured with empty user name and password fields!

Allowed Users and Available Users

Enter a straightforward name that will identify a user group in the Allowed Users text box. Click the Add button. The name will display in the Available Users box. Once the name has been accepted, you can delete it at any time.

Add Users

A list of all users who are allowed to access the SOCKS Proxy can also be configured by selecting the users from the right selection box and clicking the Add button. These users can also be added by checking the checkbox against SOCKS users in the User Authentication > Users section. The left box contains SOCKS users and the right box consists of all the local users who are not allowed to access SOCKS.

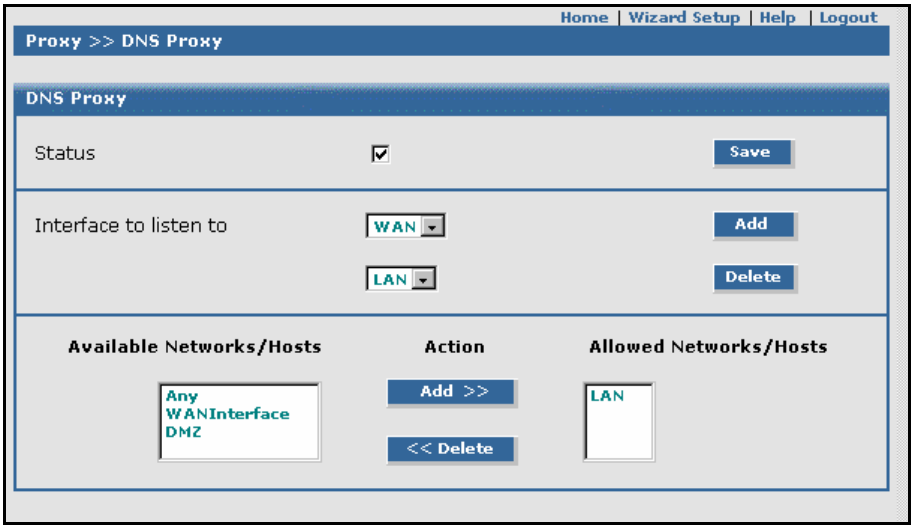
Delete Users

The users who are now allowed to access the SOCKS Proxy can be changed by selecting the users from the left box and clicking the **Delete** button. These users can also be deleted by unchecking the checkbox against SOCKS users in the **User Authentication > Users** section. The left box contains SOCKS users and the right box consists of all the local users who are not allowed to access SOCKS.

Proxy › DNS Proxy

DNS Proxy is a module used to redirect DNS requests to name servers. This module supports a caching-only name server which will store the DNS entries for a specified item. So, when there is a query next time, the values will be taken from the cache and the response will be sent from the module itself. This will shorten the waiting time significantly, especially if it is a slow connection.

On this screen you can enter the DNS (Domain Name Server) Proxy for your RouteFinder and configure it.
Note: If you configure several name servers, the servers are queried in the listed order.



DNS Proxy

Status

To enable the DNS proxy, check the DNS Status box. Click the **Save** button.

Interface to Listen To

Select the Interface option from the drop down list box. Options include **LAN**, **WAN**, and **DMZ**. Click the Add button. Your choice will display in the box under the selection list. It you want to change or delete and interface, highlight the name and click the **Delete** button.

Available Networks

This lists all the networks which are defined under Networks & Services > Networks. Select the one you want to be available for the DNS proxy. Click the **Add** button after highlighting your choice.

Allowed Networks

This is a list of all the networks which are allowed to access the DNS proxy. Any other requests are not forwarded to the DNS proxy.

Note: You can delete these networks at any time.

Network Setup

The Network Setup menus consist of Interface, PPP, PPPoE, DHCP Client, Dynamic DNS, Routes, Masquerading, SNAT, and DNAT screens. With the help of DNAT and SNAT, the destination and source address of the IP packets are converted. With **Masquerading** you can hide private networks from the outside world behind one official IP address.

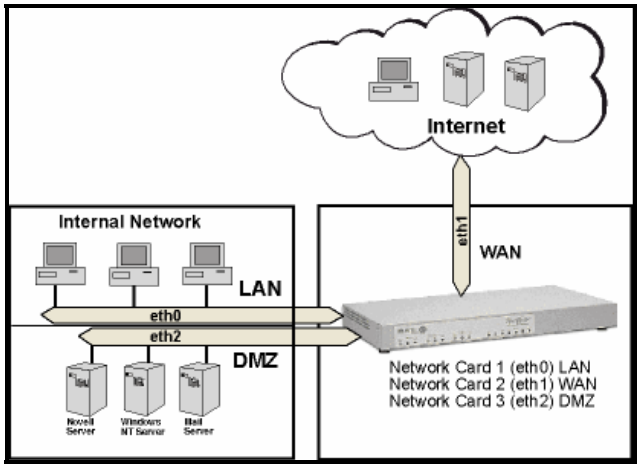
About Interfaces

During initial installation, the RouteFinder automatically recognizes the installed network card and adds them to the configuration.

Important: To change to an earlier configuration that you had saved, the RouteFinder must be re-installed. Use the **Tracking > Backup** function to read in the configuration you had set for the RouteFinder after the new installation.

The RouteFinder must be the interface between the LAN and the Internet. All information packets must pass through the RouteFinder.

We strongly recommend that you NOT put the interfaces of the RouteFinder physically together on one network segment via a hub or a switch, unless the segment is configured as a VLAN switch. To do so can lead to faulty ARP (Address Resolution Protocol) resolutions (ARP clash). Some operating systems (e.g., Microsoft Windows) cannot cope with this. That is why one network interface should be used per physical segment.



About the Interfaces Screen

The first network card (eth0) is always the interface to the internal network (LAN). It is called the **trusted** network.

The second network card (eth1) is the interface to the external network (Internet). It is the **untrusted** network.

The RouteFinder must have at least these two networks active to protect separate networks or network segments from each other.

> **Example**: The network cards could be connected in the following way:
> Network card 1: INTERNAL (to the local network)
> Network card 2: EXTERNAL (to the Internet)
> Network card 3: DMZ1 (DMZ for server)

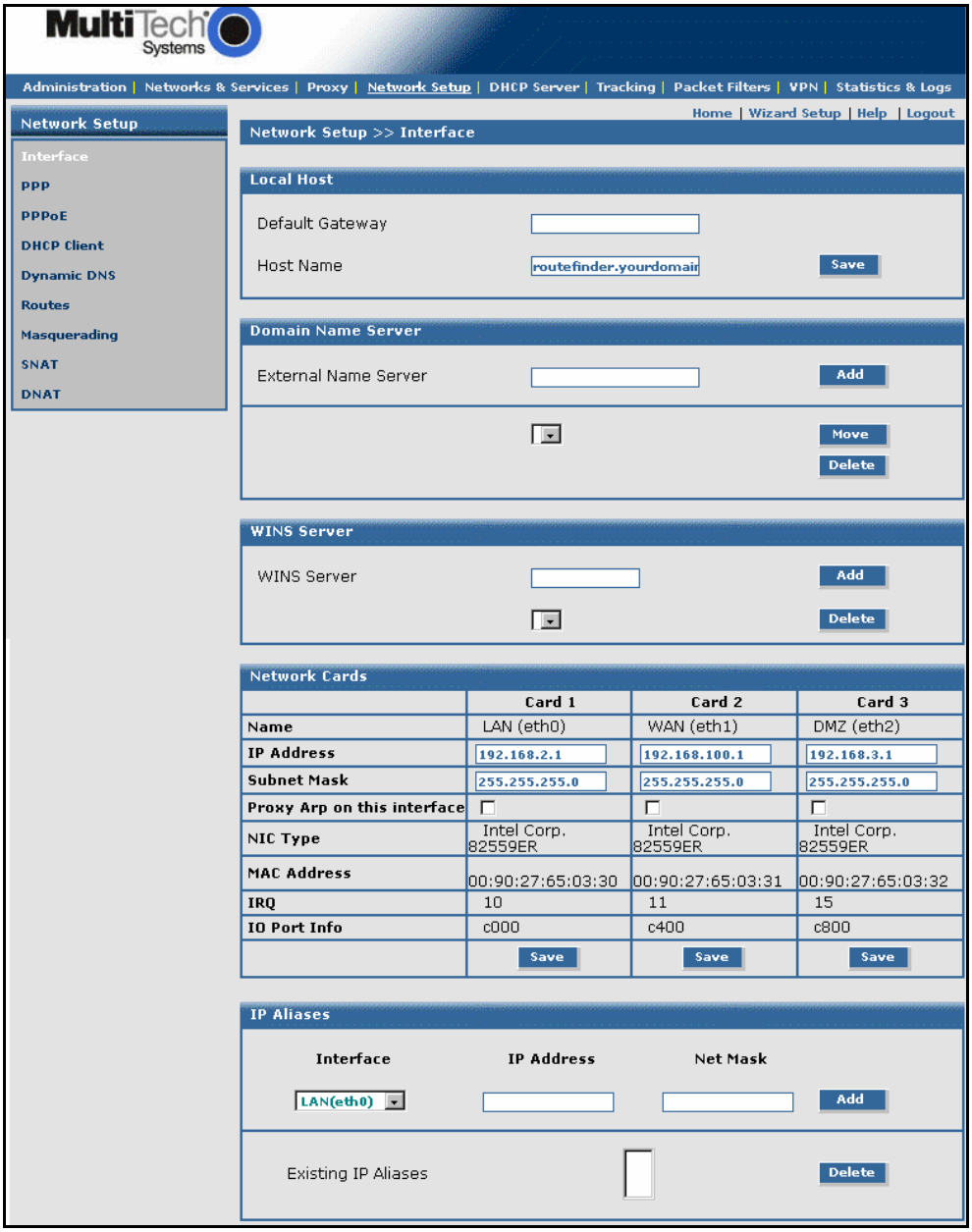
The host name and the default gateway must only be defined once. The host name is, for example, **FIREWALL.yourdomain.com**; the gateway could be your Internet router.

A suitable IP address must be entered for each network card. Let's assume that you are using a Class-C network for your internal network, in this case the entry for network card 1 could look like the following:

> Description: INTERNAL
> IP address: 192.168.2.1 (Default)
> Net mask: 255.255.255.0 (Default)

The description is for clarity purposes and is used in all further configurations. Make sure that the RouteFinder IP address is entered as the default gateway in the protected networks.

Network Setup › Interface



Local Host

Default Gateway and Host Name

The Default Gateway and the Host Name must be defined for your RouteFinder. The Default Gateway was already set during initial installation. Click the **Save** button after entering the Host Name.

Notes:

- If the gateway address and DNS addresses are assigned by a PPPoE server or a DHCP server or through a backup link, the value cannot be changed.
- The same IP Address cannot be entered for two different interfaces.

Domain Name Server

External Name Server

Enter a name for the Domain Server. Click the **Add** button. The name displays in the box just under this field. Once the name is in this box, you can highlight it and delete it or move it

WINS Server

WINS Server

Enter a name for the WINS Server. Click the **Add** button.

Network Cards

About Network Card 1 (LAN eth0)
Network Card 1 is the interface to the internal network (LAN). The information was entered during initial installation. This can be changed.

About Network Card 2 (WAN eth1)
Network Card 2 is the interface to the external network (Internet). This network card (**eth1**)

About Network Card 3 (DMZ eth2)
This network card (eth2) is the interface to the optional DMZ network. A DMZ (De-militarized Zone) is a special LAN on the public network side of a firewall to allow a single WAN router to support both private (VPN) and public access to resources. Using a DMZ allows one IP Address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. A DMZ allows just one computer to be exposed for that purpose. It is recommended that you set your computer with a static IP to use DMZ.

Effect of Changes
When you make a change that affects other administration functions and configurations, an informational screen displays. It tells you that the network interface you have just changed is used in several other configurations, and then the configurations affected by this change are listed for you. If the automatic changes are acceptable, continue editing. If the automatic changes are not acceptable, click your browser's **Back** button and continue.

Name
Enter a definition of the network card into the Name entry field.

IP Address and Subnet Mask
Enter the IP address and the corresponding Subnet Mask into the appropriate entry fields. For example:

Network Card 1 (LAN eth0)	*Network Card 2 (WAN eth1)*	*Network Card 3 (DMZ eth2)*
Name (Description): LAN IP Address: 192.168.2.1 Subnet Mask: 255.255.255.0	Name (Description): WAN IP Address: 192.168.100.1 Subnet Mask: 255.255.255.0	Name (Description): DMZ IP Address: 192.168.3.1 Subnet Mask: 255.255.255.0

Caution: When entering a new IP address for Network Card 1, it is possible to "lock yourself out". If you do, in most cases you will need to reinstall the RouteFinder to re-establish access.

Proxy ARP on This Interface
If you check the **Proxy ARP on This Interface** checkbox, the RouteFinder will automatically announce itself as responsible for all packets to destinations for which it has an Interface Route. You can use this function to "half-bridge" a network into another LAN segment.

Note: All packet filtering rules still apply when Proxy ARP is enabled. This is not a full bridging function!

If the Proxy ARP on This Interface function is activated, the RouteFinder will relay the ARP protocol on this network card for all the networks known to it. This means that the RouteFinder will accept and forward packets on the Proxy ARP interface for all other directly connected networks.

This function is necessary in some special cases; e.g., when the correct routes for a network cannot be set and the network has to be passed on through the firewall. This can be the case if you have no access to the router of your Internet provider.

A Possible Error: The Interfaces menu doesn't contain entry fields for all the network cards.
Possible Cause of Error: The missing network card was added after the installation of the RouteFinder, or it wasn't recognized during installation.
Solution: Reinstall the RouteFinder software. You can use the backup feature (described earlier in this chapter) to transfer your configuration between the installations.

NIC Type, MAC Address, IRQ, and IO Port Info
This information defaults into the corresponding fields.

Save
Confirm your settings by clicking the **Save** button.

IP Aliases

From this part of the Interfaces screen you can add RouteFinder network interface IP Aliases. IP aliases can be used to assign additional IP addresses to a network card. The RouteFinder will treat the additional addresses as equals to the primary network card addresses. IP aliases are required to administer several logical networks on one network card. They can also be necessary in connection with the SNAT function to assign additional addresses to the firewall. Up to 100 additional addresses can be configured on each network card.

Interface
From the drop down list box, select the network name to which you want to assign an alias.

IP Address
Enter the network IP address for the network named.

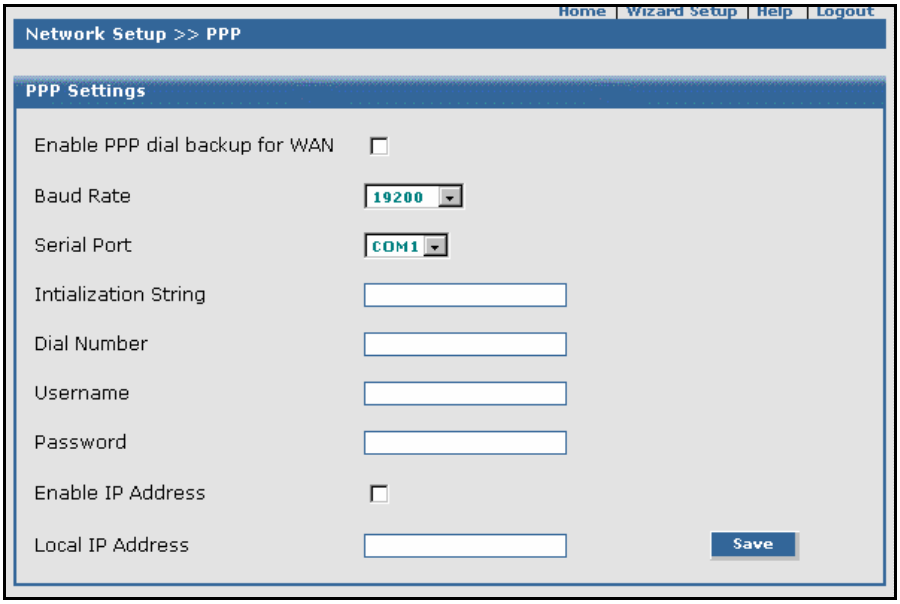
Netmask
Enter the Netmask to be used for this network.

Save
Click the **Save** button.

Delete IP Alias
An IP alias is deleted by highlighting it in the table and then clicking the **Delete** button.

Network Setup › PPP

The PPP link is used as a backup link to the WAN interface. If the PPPoE or static link goes down, the backup link will automatically come up and the system will be again connected to the ISP. On this screen you can set up PPP dial up backup for your WAN interface.



PPP Settings

Enable PPP Dial Backup for WAN – To enable PPP Dial Backup for WAN, check the corresponding checkbox.

Baud Rate – Select the baud rate from the drop down list box. Options: 9600, 19200, 38400, 57600, and 115200.

Serial Port – Select the Serial Port from the drop down list box. Options: COM1 and COM2; use COM2.

Initialization String – Enter the set of commands you want sent to the modem at startup. The initialization string sets speed, error correction, compression, various timeout values, and how to display results to the user. You can also change your country or region code by including the country/region code AT command in the initialization string (see directions below).

Dial Number – Enter the phone number that the modem will use to connect to the PSTN.

User Name – Enter the ISP User Name designated for dialup access.

Password – Enter the ISP Password designated for dialup access; the password is optional.

Enable IP Setting – Check this box to enable the IP setting. This option can be set to make the firewall negotiate for a particular IP address from the ISP.

Local IP Address – If the checkbox **Enable IP** is checked, the IP address has to be entered in this field.

Save – Click **Save** to activate these settings.

Change Your Country/Region Code

To change the country/region code, the **initialization string** must contain the AT command for your specific country or region.

1. Type **AT%T19,0,*nn***, where ***nn*** is the country/region code in hexadecimal notation.
   Click **Enter**.
   OK displays.
2. To verify that the correct country/region has been configured, type:
   ATI9 and click **Enter**.
3. The country/region code displays:

Example:	*Country/Region*	*AT Command (hexadecimal)*	*Result code (decimal)*
	Euro/NAM	AT%T19,0,34 (default)	52

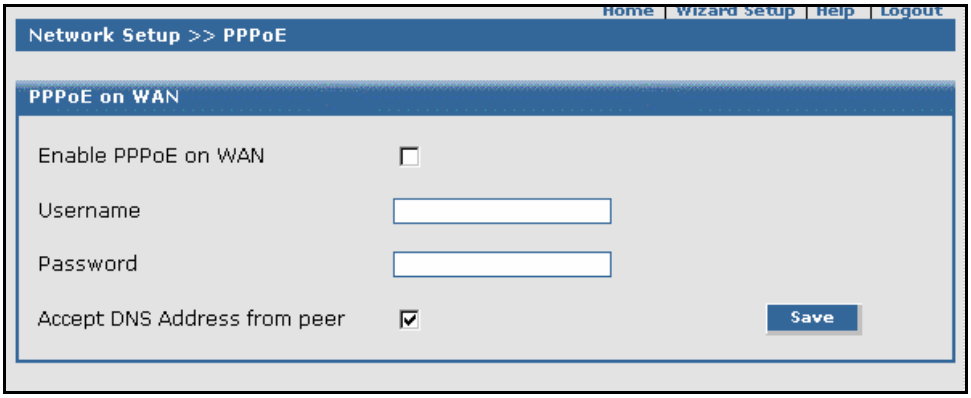
A list of country/region codes can be found on the Multi-Tech Web site at

http://www.multitech.com/PRODUCTS/Categories/Modems/global/configuration.asp#chart

Network Setup › PPPoE

PPPoE (Point-to-Point Protocol over Ethernet) is a specification for connecting multiple computer users on an Ethernet local area network to a remote site through DSL or cable modems or similar devices. PPPoE can be used to have an office or building-full of users share a common Digital Subscriber Line (DSL), cable modem, or wireless connection to the internet. PPPoE combines the Point-to-Point (PPP), commonly used in dialup connections, with the Ethernet protocol which support multiple users in a local area network.

Important: If DHCP client is enabled, the PPPoE cannot be used. The internet connection can be either PPPoE or DHCP client at any given time.



PPPoE on WAN

Enable PPPoE on WAN
To Enable PPPoE on WAN, check the corresponding box. This will enable the interface connected to the ADSL modem (this will be the interface to the internet).

User Name
This field defines the ADSL User Name given by the ISP.

Password
The user's password must be entered in this field.

DNS Address from Peer
Check this box if you want to obtain DNS server addresses from the peer (i.e., the ISP).

Save
Click **Save** to activate these settings.

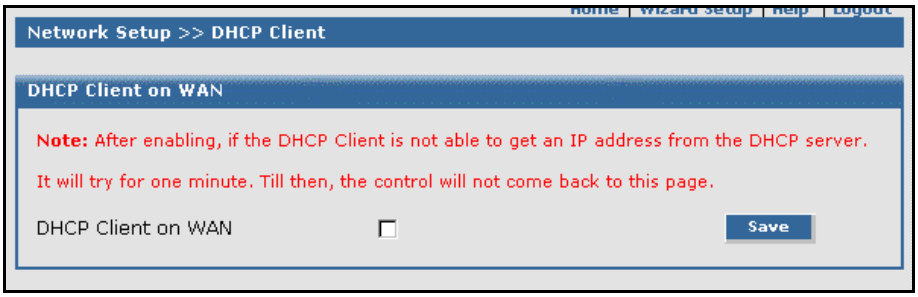
Network Setup › DHCP Client

On this screen you can enable DHCP Client (Dynamic Host Configuration Protocol), which is a TCP/IP protocol that enables PCs and workstations to get temporary or permanent IP addresses out of a pool from centrally-administered servers. This screen will provide user messages such as the one shown is red. Later, it will display the Current DHCP Client Status. For example: DHCP Client has not yet obtained an IP address from the DHCP server.

Important: If PPPoE is enabled, then DHCP client cannot be enabled. The interface to the internet can be either through PPPoE or DHCP client at any time.

If DHCP client is enabled and if the IP address has been assigned, then the following values will be displayed on this screen:

- Assigned IP Address
- Mask
- DHCP
- DNS Address
- Gateway Address
- Renew Time (time at which the DHCP client should begin trying to contact its server to renew the lease it has obtained).
- Expiry Time (time at which the DHCP client must stop using the lease if it has not been able to contact a server in order to renew it).



DHCP Settings

DHCP Client on WAN

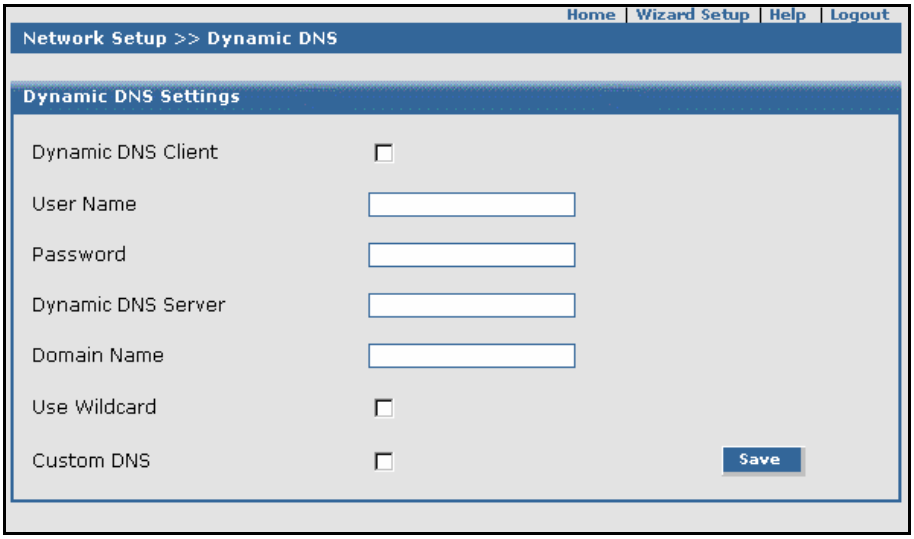
To Enable DHCP Client on WAN, check the corresponding checkbox.

Save

Click the **Save** button after enabling this function.

Network Setup › Dynamic DNS

Dynamic DNS allows a user to connect his PC to the Internet with a dynamic IP address, so that he will be able to use applications that require a static IP address.



Dynamic DNS Settings

Dynamic DNS Client

Check the box to enable Dynamic DNS Client for this machine.

User Name

Enter the name or the email ID you have specified while registering with the Dynamic DNS server.

Password

Enter the password you had specified while registering with the Dynamic DNS server.

Dynamic DNS Server

Enter the server to which you have registered for dynamic DNS service.
At present, only the following servers are supported for this function:

1. dyndns.org
2. zoneedit.com
3. easydns.com
4. hn.org
5. dslreports.com
6. dnspark.com

Domain Name

Enter the domain name which you have registered with the Dynamic DNS server.

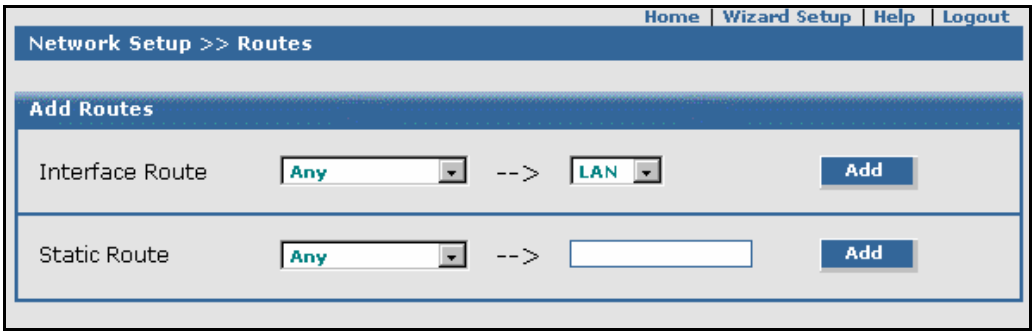
Use Wildcard

If you enable this option, subdomains of the domain you have registered will also be resolved to the same IP address.
For example, if you have registered *test.dyndns.org*, and the IP address assigned to it is resolved to *a.b.c.d*, all the subdomains (e.g., *dns.test.dyndns.org*) will also be resolved to *a.b.c.d*.

Network Setup › Routes

Routing information is used by every computer connected to a network to identify whether it is sending a data packet directly to the Firewall or passing it on to another network. There are two types of routes used by the firewall, interface routes that describe routing entries for directly connected networks and static routes that describe routes which are to be routed using a secondary router. You can add and delete entries in both these type of routes.

The RouteFinder itself adds routing entries for directly connected networks. These routes are called Interface Routes. Further entries for networks in which the RouteFinder itself is NOT a member must be made manually (e.g., if there is a second router on the network and a particular network is to be routed to it, for example if the second router is to be responsible for this network).



Add Routes - Interface Route

Interface Route

Select an already defined network and a network card. The entries are confirmed by clicking the **Add** button. Also, existing entries can be deleted by highlighting the entry and clicking the **Delete** button.

Note: While adding a route, if the network cannot be reached through that interface, the route will not be added.

Add Routes - Static Route

This selection defines networks that are not directly connected, but are connected through a secondary router or gateway. Select an already defined network for the drop-down list. Enter the external IP address which will act as a gateway for this network. Confirm your entry by clicking the **Add** button. Existing entries can be deleted by highlighting the entry and clicking the **Delete** button.

Note: The specified gateway should be reachable first. This means that a static route should already be configured for the gateway.

Delete a Route

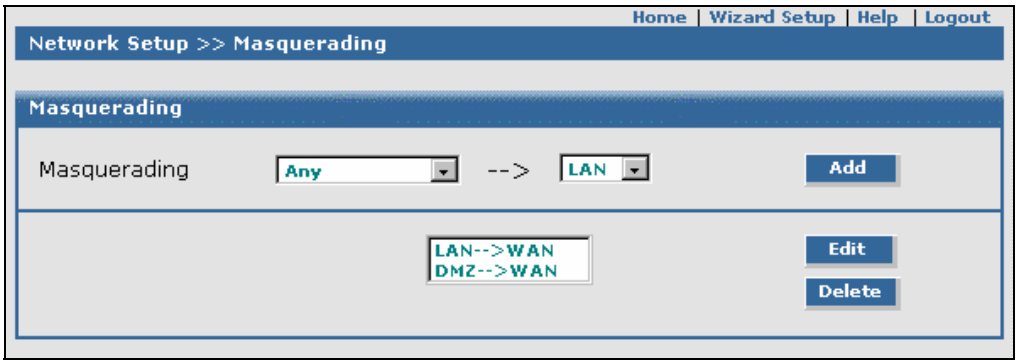
Select a Route from the table and click the **Delete** button. When deleting a Route, the interface adapts accordingly.

Note: You can view the Routing Table in **Statistics & Logs > Networks > Routing Table**.

Network Setup › Masquerading

Masquerading is a process which allows a whole network to hide behind one or several addresses preventing the identification of your network topology from the outside. Masquerading enables the user to enter only one source network. All services are automatically included in the transition. The translation takes place only if the packet is sent via the indicated network interface. The address of this interface is used as the new source of the data packets.

On this screen you can select networks or network groups to be masked to selected network cards. Masquerading is especially useful for connecting private networks to the Internet. It allows you to hide internal IP addresses and network information from the outside network.



Masquerading

Masquerading

Select one of the networks already defined in the Networks menu. Select a network from each box (***from*** and ***to*** networks).

Add

Click the **Add** button. The Masqueraded network route displays below.

Edit or Delete a Route

Select Masqueraded network route from the lower box and click the **Edit** or **Delete** button. When deleting a Masqueraded network route, the interface adapts accordingly.

Example

In this example, the sent packet does not contain any internal information. The reply to the request is recognized by the RouteFinder and is passed on to the requesting computer.

Computer A with the address XY is inside a masked network within the RouteFinder.

It starts an HTTP request into the Internet. Computer A - and all computers in this network - use the only official IP address. For all data packets that are to go into the Internet, the IP address of the sender is exchanged for the IP address of the external network card.

Network Setup › SNAT

The SNAT (Source Network Address Translation) process allows attaching private networks to public networks. SNAT is used when you want to have a LAN using a private IP network to be connected to the internet via a firewall. Since the private IP addresses are not routed on the internet, you have to apply SNAT on the firewall's external interface.

The firewall's internal interface serves as the default gateway for the LAN. Hence, a rule is added to the firewall to replace the source address of all packets crossing the firewall's external interface from inside to outside with the firewall's own IP address. Once the request gets answered from the Internet host, the firewall will receive the reply packets and will forward them to the client on the LAN.

On this screen you can set up the RouteFinder's ability to rewrite the source address of in-transit data packages using SNAT. This functionality is equivalent to DNAT, except that the source addresses of the IP packets are converted instead of the target addresses being converted. This can be helpful in more complex situations (e.g., diverting reply packets of connections to other networks or hosts).

Important

For SNAT support, the TCP and/or UDP settings must be enabled at **Networks & Services > Services > Protocol**.

Important

As the translation takes place after the filtering by packet filter rules, you must allow connections that concern your SNAT rules in **Packet Filters > Packet Filter Rules** with the original source address. Packet filter rules are covered later in this chapter.

Note: To create simple connections from private networks to the Internet, you should use the **Network Setup > Masquerading** function instead of SNAT. In contrast to Masquerading, SNAT is a static address conversion, and the rewritten source address does not have to be one of the RouteFinder's IP addresses.

Add SNAT Definition

From the drop down list boxes, select IP packet characteristics to be translated. The options are:

Pre SNAT Source

Select the original source network of the packet. The network must be predefined in the **Networks** menu. The entry is confirmed by clicking the **Add** button. Existing entries can be deleted or edited by clicking the **Edit** or the **Delete** buttons.

Service

Allows the corresponding service for the Pre SNAT Source entry field to be chosen from the select menus. The service must have already been defined in the **Services** menu.

Destination

Select the target network of the packet. The network must have been defined in the **Network** menu. The entry is confirmed by clicking the **Add** button. Existing entries can be deleted or edited by clicking the **Edit** or the **Delete** buttons.

Post SNAT Source

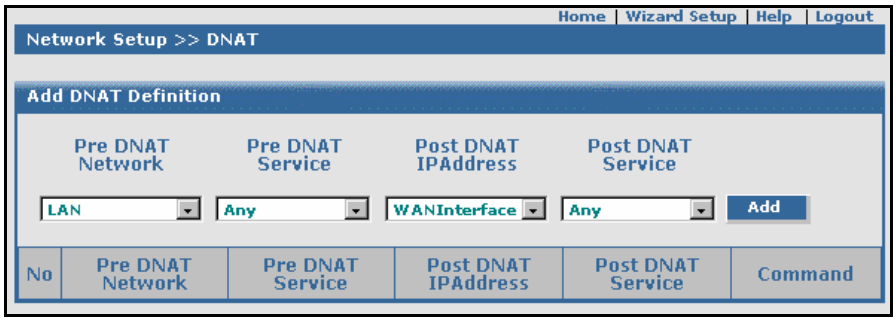
Selects the source addresses of all the packets after the translation. Only one host can be specified here. The entry is confirmed by clicking the **Add** button. Existing entries can be deleted or edited by clicking the **Edit** or the **Delete** buttons.

Network Setup › DNAT

On this screen you can set up DNAT re-routing. DNAT (Destination Network Address Translation) describes the target addresses of the IP packets. Use DNAT if you want to operate a private network behind your RouteFinder firewall and provide network services that run only behind this private network available to the Internet. Note that for DNAT support, the TCP and/or UDP settings must be enabled (at **Networks & Services > Services > Protocol**).

Important Notes:

- You **cannot** add a DNAT rule with the Pre DNAT Network as ANY, with Service as ANY, and a Destination Service as ANY. All the packets will be routed to the system with Post SNAT network, and then the services in the firewall will not function properly.
- As the address conversion takes place BEFORE the filtering by the packet filter rules, you must set the appropriate rules in the **Packet Filter > Rules** menu to let the already-translated packets pass. You can find more about setting packet filter rules earlier in this chapter.



Add DNAT Definition

The DNAT screen contains four drop down list boxes. The first two define the original target of the IP packets that are to be re-routed. The last two define the new target to which the packets are forwarded. From the drop down list boxes, select IP packet characteristics to be translated.

Pre DNAT Destination

Select the target host or target network (e.g., PPTP-Pool) and the corresponding Service (e.g., DNS, FTP, FTP-CONTROL) to be redirected. Note that a network can consist of one single address with net mask 255.255.255.255.

Post DNAT Destination

Select a host to which the IP packets are to be diverted. Only one host can be defined as the Post DNAT destination.

Important: If you are using a port range as the Post DNAT Service, you must enter the same Service definition as you entered in the Pre DNAT Service. In other words, you can only map one port range to the same port range. Select a corresponding Service (e.g., DNS, FTP, FTP-CONTROL) to be redirected.

Add, Edit, Delete

Click the **Add** button to save your choices. After saving the settings, a table is created. You can edit or delete entries by highlighting the desired entries and clicking either the **Edit** or **Delete** button listed under ***Command***.

DNAT Example

Your Internet/private network has the address range 192.168.0.0/255.255.255.0. You now want to make a Web server that is running on port 80 of the server with the IP address 192.168.0.20 accessible to clients outside your LAN. These clients cannot contact its address directly, as the IP address is not routed in the Internet. It is, however, possible to contact an external address of your RouteFinder from the Internet. With DNAT, you can re-route port 80 on the RouteFinder's external interface onto the Web server.

Note: To divert port 443 (HTTPS), you must change the value of the TCP port on the **Administration > Administrative Access** screen in the field **Administrative Access HTTPS Port** (e.g., port 444).

Examples of DNAT Network Combinations

You can map:

- IP/Port ⇒ IP/Port
- IP/Port-Range ⇒ IP/Port
- IP/Port-Range ⇒ IP/Port-Range (only if the Port-Range is the same for PRE and POST)
- IP-Range/Port ⇒ IP/Port
- IP-Range/Port-Range ⇒ IP/Port

You cannot map:

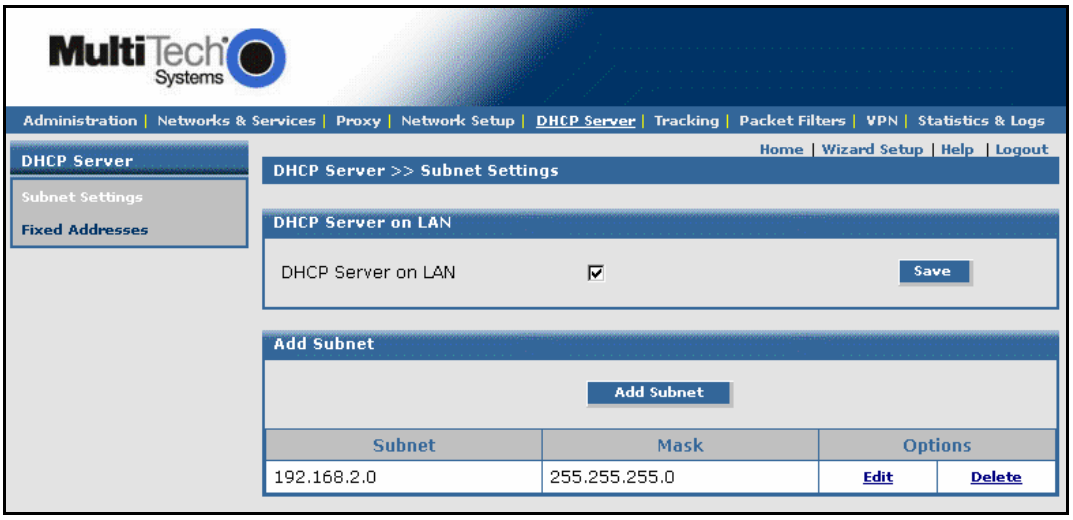
- IP ⇒ IP
- IP-Range ⇒ IP
- IP-Range ⇒ IP-Range
- IP ⇒ IP-Range (load balancing)

The "way back" (return) translation is done automatically; you do not need a rule for it.

DHCP Server

DHCP Server › Subnet Settings

DHCP (Dynamic Host Configuration Protocol) is a protocol which allows individual devices on an IP network to get their own network configuration information (IP address, subnetmask, broadcast address, etc.) from a DHCP server. The overall purpose of the DHCP is to make it easier to administer a large network. The DHCP package includes the DHCP server and a DHCP relay agent.



DHCP Server on LAN

DHCP Server on LAN

The DHCP Server is enabled by default. If you would like to disable it, uncheck the DHCP Server on LAN checkbox. If you change the check mark, click the **Save** button to activate the change.

Add

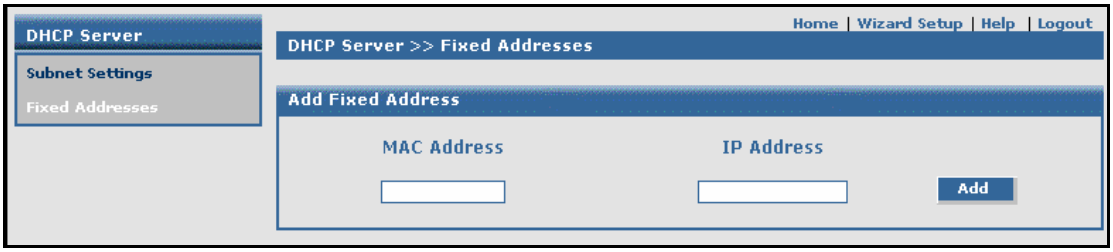
Click the **Add Subnet** button which will open the table for entering the Subnet IP Address and Mask.

Edit or Delete

You can edit or delete entries by selecting the desired entries and clicking either the **Edit** button or **Delete** button listed under **Options**.

DHCP Server › Fixed Addresses

The DHCP server can be made to assign a fixed IP address for a particular user by identifying the MAC address. This binding can be made permanent by configuring the same using this screen. The same IP address would not be used for any DHCP client with a different MAC address, even if there is no active DHCP connection with that IP address.



DHCP Server Fixed Addresses

Add Fixed Address

Enter both a MAC address and an IP address.

Tracking

Tracking › Accounting

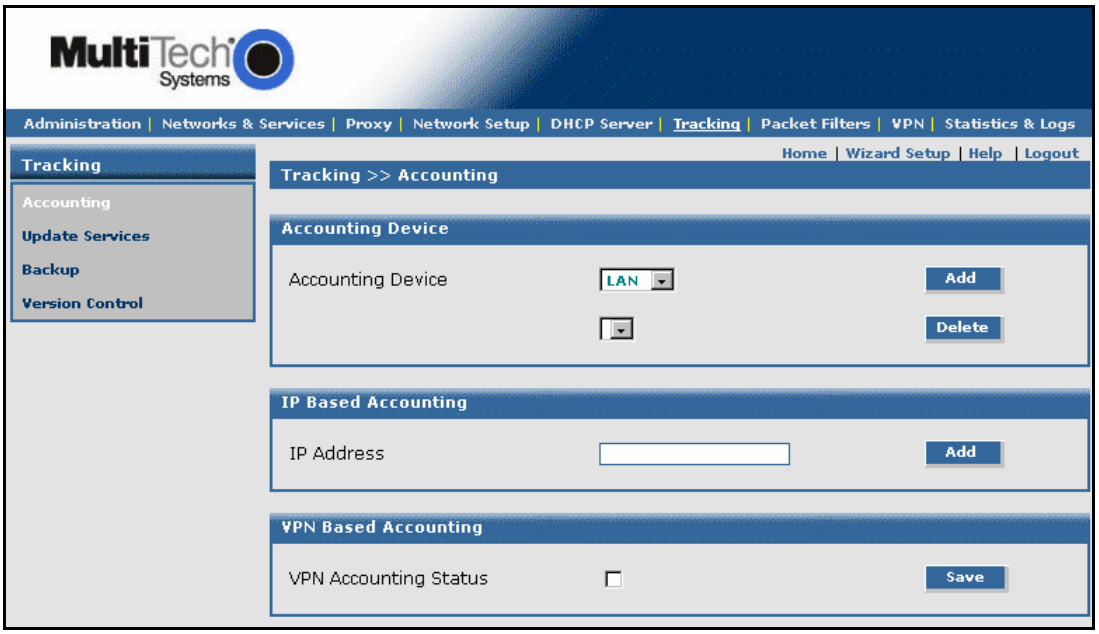
The Accounting function records all the IP packets on the external network cards and sums up their size. The traffic sum for each day is calculated once a day. Additionally, the traffic sum for the current month is calculated and displayed. This is the amount that your ISP (Internet Service Provider) will charge to you if your payment plan is based on the amount of data you transfer.

On this screen you can specify which local devices will have their network traffic counted and recorded. You can also exclude hosts or networks from the accounting process.

After this accounting is in place, you can view the Accounting of your RouteFinder in the **Statistics & Logs > Accounting** menu.

You can also exclude Hosts or Networks from Accounting. After installing your RouteFinder, all networks are included in the accounting function. Excluding a network from Accounting could be useful if the interface to the DMZ is entered in the Accounting while one particular computer in the DMZ is not to be accounted. If this one computer is only to be used for internal purposes, it does not make sense to include its information traffic in the accounting balance.

Note: The traffic will be displayed as graphs in **Statistics & Logs > Accounting**.



Accounting Device

Accounting Device

From the Accounting Device drop down box, select the network to have its traffic counted. The options are **LAN**, **WAN**, and **DMZ**. Click the **Add** button to confirm your entry. After the entry is completed, a table for this network is created.

IP-Based Accounting

IP Address

Enter the IP addresses for which traffic is to be monitored. The traffic to and from the particular IP address destined to one of the firewall's interfaces and the traffic to and from the particular IP address and forwarded by the firewall will be considered for accounting. Click the **Add** button.

VPN Accounting

VPN-Based Accounting

Check the VPN Accounting Status box to have the VPN status monitored by the accounting function. Click the **Save** button.

Tracking › Update Services

On this screen you can define RouteFinder update parameters. If you use the Update Service, your RouteFinder can be continually updated with new virus protection patterns, system patches, security features, and new features. The Updates are signed and encrypted and read in via an encrypted connection.

System Update Server

Server Name and Directory

Enter the name or IP address of the server you want to specify as the system update server and enter the path to this server. Click the **Save** button.

Virus Update Server

Server Name and Directory

Enter the name or IP address of the server you want to specify as the virus database update server and enter the path to this server. This process downloads and installs new virus detection patterns for the firewall's virus scanner. To ensure that patterns stay up-to-date at all times, the process can be automated by setting a time interval after which the system automatically checks for virus pattern updates at the specified update server.

Update Services

Update System, Update Virus Patterns, Update URL Categories Database

This section of the screen allows you to start the update processes of these services. Click the **Start** button to start the **Update System**, **Update Virus Patterns**, and/or **Update URL Categories Database** processes.

Note that the Current Version and Updates displays automatically.

Time Interval for Automatic Update of Virus Patterns

Your RouteFinder can be continually updated with new virus patterns (with optional email virus scan subscription), system patches, and security features that can be automatically read into your running system. The updates are signed and encrypted and read in via an encrypted connection. To setup an automatic virus update function, check the **Enable Update** checkbox. Then select the time interval after which the system automatically checks for the virus pattern updates at the specified update server. The time intervals are hourly, daily, weekly, and monthly.

Time Interval for Automatic Update of URL Categories

Your RouteFinder can be continually updated with new URL categories. To setup an automatic URL category update function, check the **Enable Update** checkbox. Then select the time interval after which the system automatically checks for URL category database updates from its server. The time intervals are daily, weekly, fortnight, and monthly.

System Update - Livelog

After clicking the **System Update - Livelog** button, a list of all downloaded packages along with the download time will be displayed.

Virus Update - Livelog

After clicking the **Virus - Livelog** button, a log file of the virus pattern updates will be displayed.

Tracking › Backup

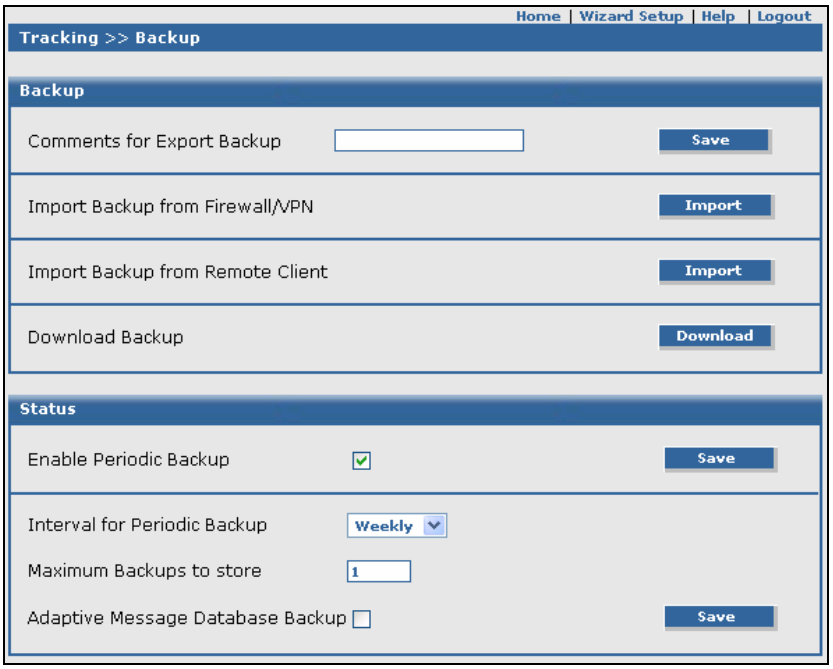
The Backup function lets you save the RouteFinder settings on a local hard disk. With a backup file, you can set a recently installed RouteFinder to the identical configuration level as an existing RouteFinder. This is useful in case there is a problem with your new settings. Also, a new RouteFinder can be installed and the backup read in minutes. This means a replacement system can be running in a very short time. The backup file contains all configuration settings except the VPN RSA Key.

The Backup function is responsible for the following:

1. Saves your firewall settings as a zip file.
2. Sends the backup as an attachment to an email to the administrator.
3. Allows you to import the backup either from the firewall or the browser machine. In this case, the settings will revert back to the settings saved in the corresponding zip file.
4. Allows you to download the backup from the firewall directly to your browser machine.

Important Notes About Backups:

- You will probably want to keep routine backups of all aspects of your RouteFinder to let you re-build it in case of an emergency, as well as to use as evidence if and when you discover a successful attack (letting you compare the before and after states of the RouteFinder).
- You may want to store all alerts and notifications.
- Passwords are saved, but the RSA key is not saved.



Backup

Comments for Export Backup

This field is a required field. Enter an explanation of the backup file for future reference. Click **Save**. This starts the backup and includes the comment as part of the backup file. The file name generated by the RouteFinder is made up of backup's date and time in the format *yyyy-mm-dd.hh-mm.zip*. The file is saved to your hard drive and can be emailed.

Caution: When reading in the backup file, the RouteFinder automatically configures itself as recorded in the backup file. For example, if IP addresses or passwords have since changed or have been forgotten, you might not be able to access the RouteFinder anymore.

Import Backup from Firewall/VPN

This function is used for restoring the configuration files from a backup file present in the firewall itself. After clicking the **Import** button, a list of all the backup files maintained in the firewall will be displayed. Select the file you want to import and click the **Get Comments** button to read the comments for this file and verify that this is the file you want. Once you are sure of the file you want, click the **Import** button. Passwords will be saved.

Note: Backups taken from a previous version cannot be imported.

Import Backup from Remote Client

When a backup is taken, the backup file is sent to the administrator through email. This function is used for restoring the configuration files from a remote client. After clicking the **Import** button, a list of all the backup files maintained on the remote client's PC display. Select the file you want to import and click the **Get Comments** button to read the comments for this file to verify that this is the file you want. Once you are sure of the file you want, click the **Import** button.

Download Backup

Click the **Download** button to backup files saved in the firewall to the local machine.

Status

Enable Periodic Backup

Place a checkmark in this box to set up an automatic performance of the periodic backups. Click the **Save** button.

Interval for Periodic Backup

Select how often you would like automatic periodic backups to be performed. Options are daily, weekly, and monthly. Then click the **Save** button.

Maximum Backup to Store

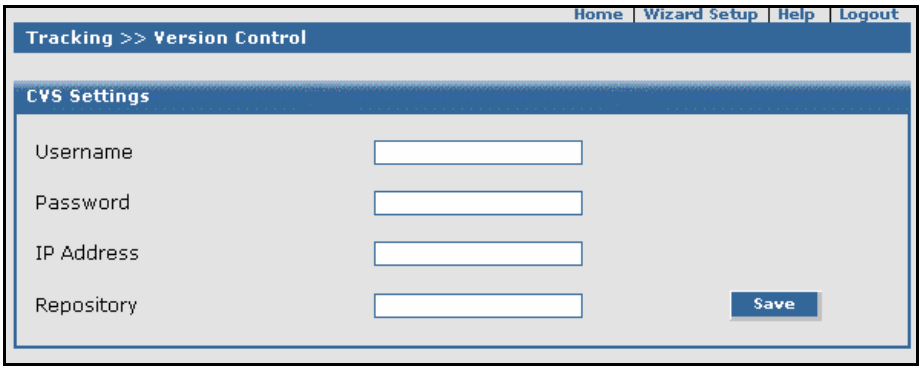
Set the maximum number of backups that you want to be retained in the server. Enter a number between 1-20.

Adaptive Database Backup

Enables Adaptive Database Backup.

Tracking › Version Control

These settings are the configuration management system settings. All configuration files can be saved in a repository in a CVS server. There are fields for setting the IP address of CVS server, user name, password, and the repository path. The corresponding user account and the directory structure should be created on the CVS server.



CVS Settings

User Name

Enter the name of the user for whom the account will be created.

Password

Enter the password for this user.

IP Address

Enter the IP address of the server where the account for the user will be created.

Repository

Enter the repository path in the server where the files can be checked in.

Examples

How to Create the CVS Server

1. Use a repository name of TEST (the repository name should always be in capital letters).
2. Let the path to the repository be: **/usr/local/cvs**
3. Create a repository in the server using the command: **cvs -d/usr/local/TEST init**

Note: A new directory cvsroot will be created under **/usr/local/cvs**.

Configuring the CVS Server

1. Add a group “CVS” to the system. Any user who needs to access the repository should be in this group.
2. Change the directory to /usr/local/cvs and set the repository’s ownership and permissions as you want them to be for this group.
3. Then change the permissions of the CVSROOT directory to ug+rwx.
4. Now create the directory TEST under usr/local/cvs.

Setting Up a CVS Password Authentication Server

1. Make sure the lines “cvspserver 2401/tcp” and “cvspserver 2401/udp” are present in:
   /etc/xinetd.d
2. Add a file named “cvspserver” containing the following information:

```
service cvspserver
{
disable = no
flags = stream
wait  = no
user = root
server = /usr/bin/cvs
server_args = -f --allow-root=/usr/local/cvs pserver
log_on_failure += USERID
log_type = FILE /root/bin/temp
}
Restart xinetd
```

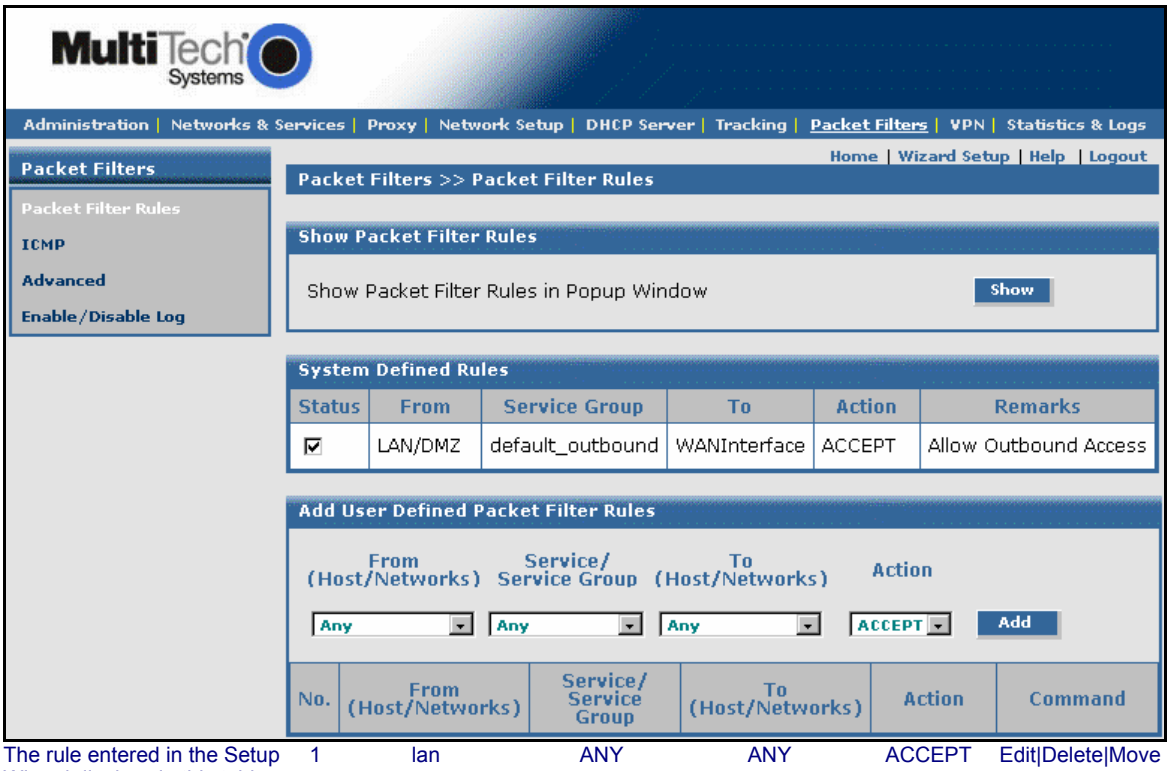
Packet Filters

Packet Filters › Packet Filter Rules

The Packet Filter is a key element of the RouteFinder. Packet filters are used to set firewall rules which define what type of data traffic is allowed across the RouteFinder's firewall. There are certain System Defined Rules that exist by default. You can specify whether particular packets are to be forwarded through the RouteFinder system or filtered. These rules are set with the help of network/host definitions and service definitions on the **Networks & Services** screen.

Prerequisites

To be able to differentiate rules, the appropriate **Networks & Services > Service Groups** and **Networks & Services > Network Groups** must first be defined.



The rule entered in the Setup Wizard displays in this table	1	lan	ANY	ANY	ACCEPT	Edit|Delete|Move

Show Packet Filter Rules in Popup Window

When you click the **Show** button, a screen displays showing the existing packet filter rules.

The RouteFinder's behavior is determined by the content and order of the filter rules. The filter rules are assigned by column number (column **nr**). Every incoming data packet is checked, in order, as to whether rule 1 is valid, rule 2 is valid, etc.) As soon as a correspondence is found, the procedure as determined by action is carried out. You can **Accept**, **Drop, Reject, Log** the packets. When packets are denied (**Rejected** setting) an entry in the appropriate log-file occurs.

All rules are entered according to the principle: **From Client** - **Service** - **To Server** - **Action**.

When setting packet filters, the two fundamental types of security policies are:

- All packets are allowed through – **Rules Setup** has to be informed explicitly what is forbidden.
- All packets are blocked – **Rules Setup** needs information about which packets to let through.

Your RouteFinder default is the all packets are blocked **setting**, as this procedure can achieve an inherently higher security. This means that you explicitly define which packets may pass through the filter. All other packets are blocked and are displayed in the **Filter LiveLog**.

Example: Network A is contained in network B.
Rule 1 allows network A to use the SMTP service.
Rule 2 forbids network B to use SMPT.

Result: Only network A is allowed SMPT.
SMPT packets from all other network B IP addresses are not allowed to pass and are logged.

Caution: Re-sorting the rules may change how the RouteFinder operates. Be very careful when defining the rule set. It determines the security of your RouteFinder.
If one rule applies, the subsequent ones are ignored. Therefore, the sequence is very important.
Never place a rule with the entries **Any – Any – Any – Accept** at the top of your rule set, as such a setting will match all packets, and thus, cause all subsequent rules to be ignored.

System Defined Rules

These rules define a set of common application services that are allowed outbound access through the RouteFinder's WAN interface. The software defines a default Service Group called ***default_outbound***. The services under ***default_outbound*** are FTP, TELNET, DNS, HTTP, POP3, IMAP, and HTTPS.

Add User Defined Packet Filter Rules

New packet filter rules are created by choosing from four drop-down lists. All services, networks, and groups previously created in **Definitions** are available for selection. Click **Add** to create the appropriate rule; it then displays at the bottom of the table. The new rule automatically receives the next available number in the table. The overall effectiveness of the rule is decided by its position in the table. You can move the new rule within the table with the **Move** function in the **Command** column.

Important:

The order of the rules in the table is essential for the correct functioning of the firewall. By clicking the **Move** button, the order of execution can be changed. In front of rule to be moved, enter the line number that indicates where the rule should be placed. Confirm by clicking **OK**.

By default, new rules are created at the end of the table.

From – Select the network from which the information packet must be sent for the rule to match. You can also select network groups. The Any option can also be given which matches all IP addresses, regardless of whether they are officially assigned addresses or so-called private addresses. These Network clients or groups must be pre-defined in the Networks menu. ***Example:*** net1 or host1 or Any

Service – Select the service that is to be matched with the rule. These services are pre-defined in the Services menu. With the help of these services, the information traffic to be filtered can be precisely defined. The default entry Any selects all combinations of protocols and parameters (e.g., ports). ***Example:*** SMTP,ANY

To – Select the network to which the data packets are sent for the rule to match. Network groups can also be selected. These network clients or groups must be pre-defined in the Networks menu.

Action – Select the action that is to be performed in the case of a successful matching (applicable filter rule). There are three types of actions:

- **Accept:** This allows/accepts all packets that match this rule.
- **Reject:** This blocs all packets that match this rule. The host sending the packet will be informed that the packet has been rejected.
- **Drop:** This drops all packets that match this rule, but the host is not informed. The action Drop is recommended for filter violations that constantly take place, are not security relevant, and only flood the LiveLog with meaningless messages (e.g., NETBIOS-Broadcasts from Windows computers). To drop packets with the target address Broadcast IP, you first have to define the appropriate broadcast address in the form of a new network in the Networks menu (defining new networks is explained in detail earlier in this chapter). You must then set and enable the packet filter rule.

To Broadcast on the Whole Internet:	*To Broadcast on One Network Segment:*
1. Open the *Networks & Services* menu, click **Add**, and enter the following data: **Name:** Broadcast32 **IP Address**: 255.255.255.255 **Subnet Mask:** 255.255.255.255 **2.** Confirm your entries by clicking the **Add** button. **3.** Open the **Rules** menu in the Packet Filter directory and set the packet filter rules: **From (Client):** Any **Service:** Any **To (Server)**: Broadcast32 **Action:** Drop **4.** Confirm your entries by clicking the **Add** button.	**1.** Open the *Networks & Services* menu, click **Add**, and enter the following data: **Name**: Broadcast8 **IP Address:** 192.168.0.255 **Subnet Mask:** 255.255.255.255 **2.** Confirm your entries by clicking the **Add** button. **3.** Open the **Rules** menu in the Packet Filter. directory and set the packet filter rules: **From (Client):** Any **Service**: Any **To (Server):** Broadcast8 **Action:** Drop **4.** Confirm your entries by clicking the **Add** button.

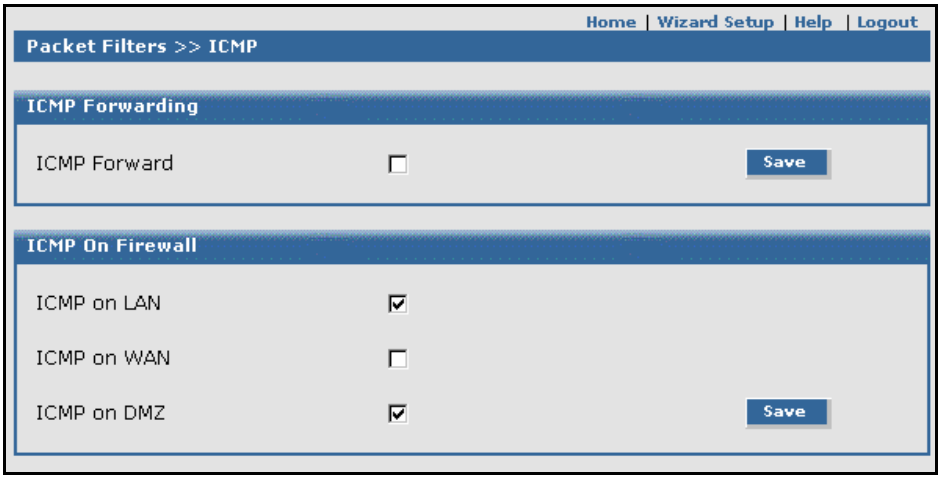
Add – Confirm your entry by clicking the **Add** button. After a successful definition, the rule is always added to the end of the rule set table. Entries can be edited by clicking the **Edit** button, which loads the data into the entry menu. The entries can then be edited. The changes are saved by clicking the **Save** button.

Delete – Rules can be deleted by clicking the **Delete** button.

Packet Filters › ICMP

ICMP (Internet Control Message Protocol) is necessary to test network connections and to test functionality of your firewall. It is also used for diagnostic purposes.

ICMP-forwarding and ICMP-on-firewall always apply to all IP addresses (“Any”). When these are enabled, all IPs can ping the firewall (ICMP-on-firewall) or the network behind it (ICMP-forwarding). Separate IP addresses can then no longer be ruled out with packet filter rules. If the ICMP settings are disabled, separate IPs and networks can be allowed to send ICMP packets through the firewall by using appropriate packet filter rules.



ICMP Forwarding

Check the ICMP Forward checkbox to enable the forwarding of **ICMP** packets through the RouteFinder into the local network and all connected DMZs. In this way you select whether an ICMP packet should be dropped or passed through to the local network and all connected DMZs.

If **ICMP forward** is enabled, ICMP packets go through all connected networks. Another use of ICMP forwarding is to allow ICMP packets to be forwarded to individual networks (set in **Packet Filter > Rules**). For this, **ICMP forward** in **Packet Filter > ICMP** must be disabled.

The status is activated by clicking the **Save** button.

ICMP on Firewall

Check the ICMP on LAN, ICMP on WAN, and/or ICMP on DMS firewall checkbox to enable the direct sending and receiving of **ICMP** packets by the RouteFinder. Then click the **Save** button.

Note: To be able to use the tools **Trace Route** and **Ping**, the function **ICMP on firewall** must be enabled. After a successful startup of the RouteFinder, it is recommended that you disable this rule so that the RouteFinder cannot be pinged anymore.

Packet Filters › Advanced

On this screen you can configure the advanced packet filter settings.

H.323 Packets Passthrough

Check this box to enable the forwarding of H.323 packets across the firewall. Click **Save**.

PPTP Packets Passthrough

Check this box to enable the forwarding of PPTP packet passthrough (PPTP NAT support). Click **Save**. This includes two features:

1. Server behind the firewall and client on the Internet. DNAT of PPTP packets.
2. Clients behind the firewall and server on the Internet. SNAT / masquerading of PPTP packets.

Private Addresses in WAN Interface

Allow Private Addresses – By default, packets from / via the WAN interface of the RouteFinder, destined to any private address, will be dropped. This option allows enabling/disabling of this feature. Click **Save** when you make a change.

Allow Strict TCP Connection Passthrough

By default, packets with invalid flag combinations or TCP sequence numbers passing via the RouteFinder will be dropped. Check the *TCP Strict* box and click the **Save** button to allow these packets to passthrough instead of being dropped. To maintain the Strict TCP connection default, do not check this box.

Drop Fragmented Packets

Dropped Fragmented Packets – Enables/disables dropping of IP fragmented packets.

Log (Dropped) Fragmented Packets – Check the *Log (Dropped) Fragmented Packets* checkbox to enable/disable the logging of dropped IP fragments by the RouteFinder firewall.

MAC Address-Based Filtering

With this option, you can filter / forward packets based on the source MAC address.

Note: MAC address-based rules will be applied to packets destined to the firewall and to packets forwarded by the firewall.

Source MAC Address – Mac Address of the source machine for which the filter rule has to be added.

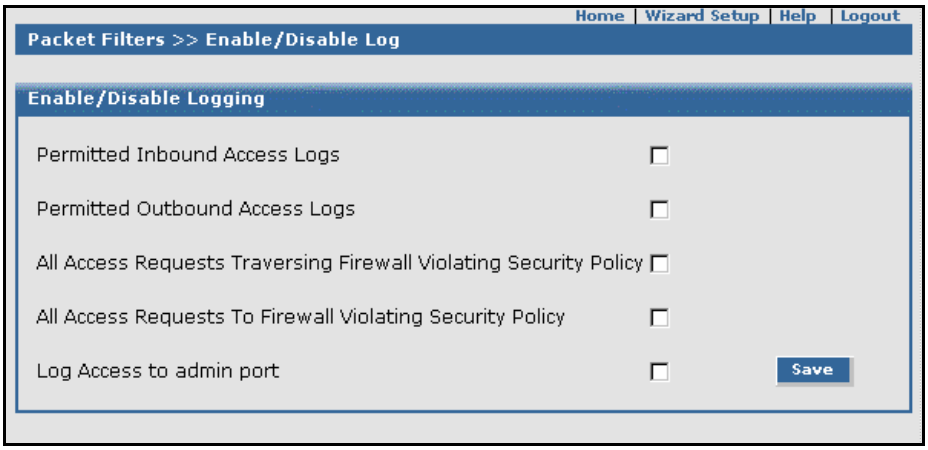
Destination IP Address – IP Address of the destination host / network for which the filter rule has to be added.

Service – The protocol – port part for which the filter rule has to be added.

Action – Select whether you want the packet to be forwarded or dropped.

Packet Filters › Enable/Disable Log

On this screen you can enable/disable RouteFinder firewall logging.



Enable/Disable Logging

Permitted Inbound Access Logs

Check this box to enable the logging of all permitted inbound access requests from public (WAN) network clients that use a service hosted on the RouteFinder itself or on a private (LAN) or service (DMZ) server/host.

Permitted Outbound Access Logs

Check this box to enable the logging of all permitted outbound access requests from private (LAN) and service (DMZ) network clients that use a service on a public (WAN) network server/host.

All Access Requests Traversing Firewall Violating Security Policy

Check this box to enable the logging of all access requests from private (LAN), service (DMZ), and public (WAN) network clients to traverse the RouteFinder that violate the configured security policy.

All Access Requests to Firewall Violating Security Policy

Check this box to enable the logging of all access requests from private (LAN), service (DMZ), and public (WAN) network clients to send traffic to the RouteFinder itself, that violate the configured security policy.

Log Access to Admin Port

Check this box to enable the logging of all access requests from private (LAN), service (DMZ), and public (WAN) network clients to send traffic to the RouteFinder itself on the administrative access port.

VPN (Virtual Private Networks)

VPN › IPSec

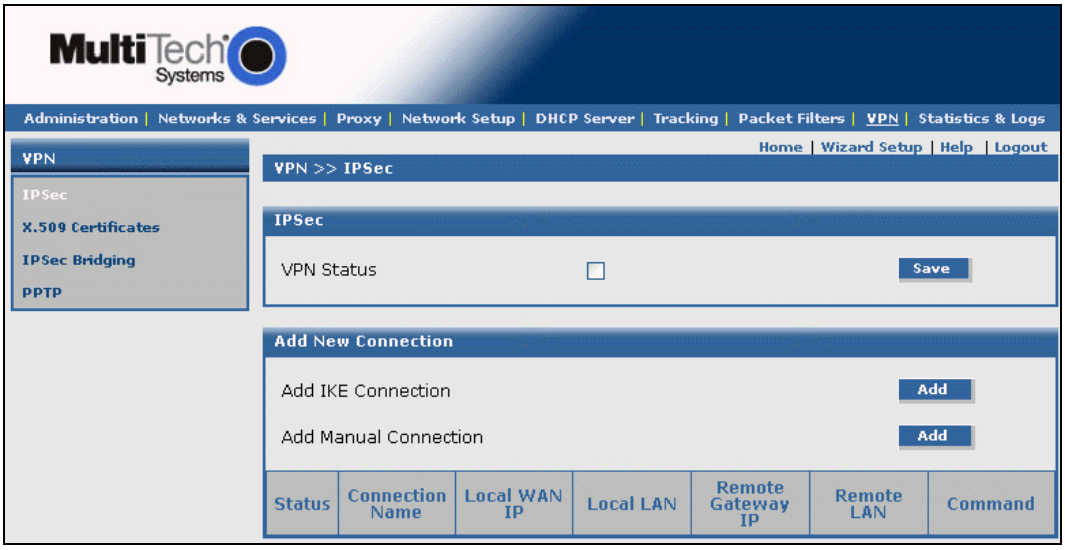
Introduction to Virtual Private Networks

A Virtual Private Network (VPN) is a secure communication connection via an insecure medium – usually the Internet. A VPN is useful in situations where information is sent and received via the Internet and it is important that no third party can read or change that information. Such a connection is secured via VPN software that is installed at both ends of the connection. This software allows authentication, key exchange, and data encryption according to an open standard (IPSec).

The IPSec protocol suite, based on modern cryptographic technologies, provides security services like encryption and authentication at the IP network layer. It secures the whole network traffic providing guaranteed security for any application using the network. It can be used to create private secured tunnels between two hosts, two security gateways, or a host and a security gateway.

Note: Scenarios for using VPN connections were illustrated in Chapter 4.

The VPN Main Screen



VPN IPSec Settings

VPN Status

Check the VPN **Status** checkbox to enable IPSec.

Click the **Save** button.

Add a New Connection

Add IKE Connection

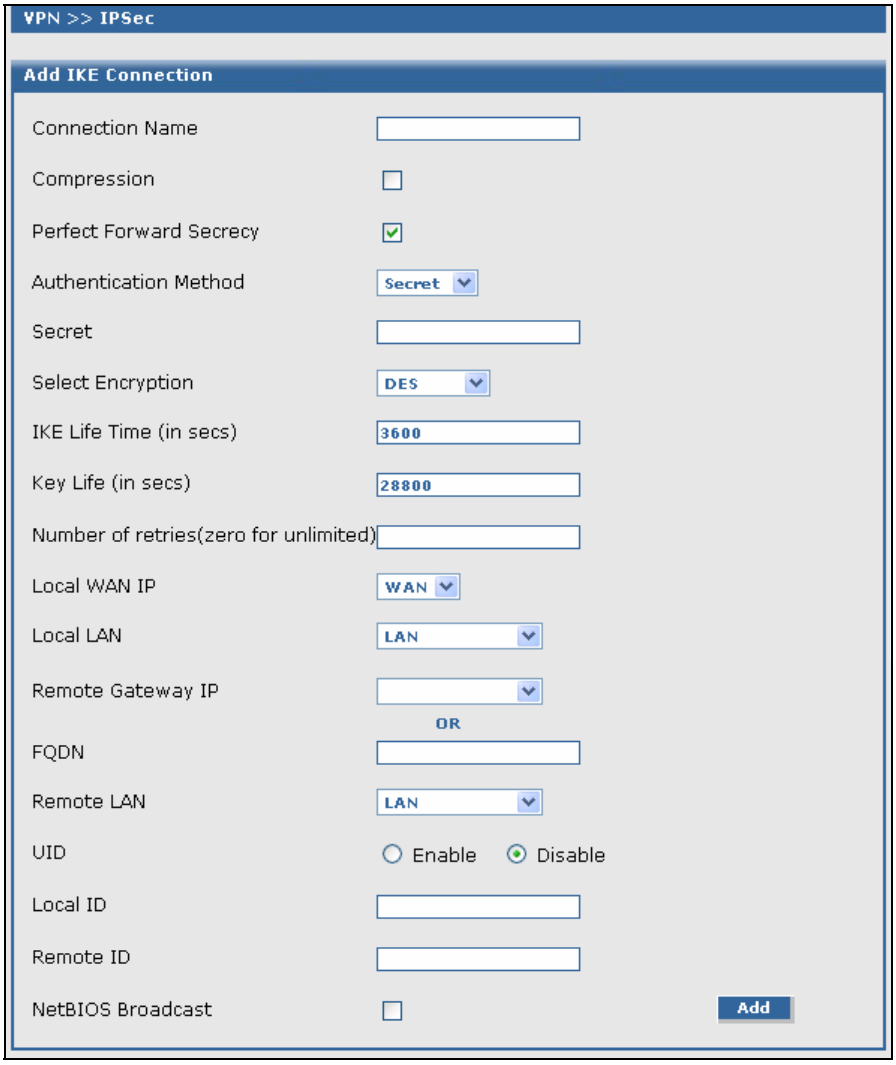
Click the **Add IKE Connection** button. A screen displays for setting up an IKE connection.

Add Manual Connection

Click the **Add Manual Connection** button. A separate screen displays for setting up a manual connection.

Add an IKE Connection

The IKE protocol automatically negotiates protocols and encryption algorithms; it keys automatic exchange of keys.



Add IKE Connection

Connection Name

Enter a text name that will identify the connection for you.

Compression

Check the compression checkbox to enable IPCOMP, the compression algorithm.

Perfect Forward Secrecy (PFS)

Check the PFS checkbox to enable PFS, a concept in which the newly generated keys are unrelated to the older keys). This is enabled by default.

Authentication Method

Check an authentication method, either Secret or RSA signatures.

Secret

If the authentication method is Secret, this field must be configured. The Secret must be agreed upon and shared by the VPN endpoints; it must be configured at both endpoints of the tunnel.

Select Encryption

Select the encryption method. 3DES is recommended.

IKE Life Time

The duration for which the ISAKMP SA should last is from successful negotiation to expiration. The default value is 3600 seconds and the maximum is 28800 seconds.

Key Life

The duration for which the IPSec SA should last is from successful negotiation to expiration. The default value is 28800 seconds and the maximum is 86400 seconds.

Number of Retries

Specify the number of retries for the IPSec tunnel. Enter zero for unlimited retries.

Local WAN IP
This is the interface initiating the IPSec tunnel.

Local LAN
Local security gateway for which the security services should be provided. If the RouteFinder acts as a host, this should be configured as **None**.

Remote Gateway IP or FQDN
Interface where the IPSec tunnel ends. In the case of a Road Warrior with a Dynamic IP address, this should be configured to **ANY**. FQDN is a DNS resolvable fully qualified domain name with which identity the right peer can be identified. When FQDN is selected, the Remote Gateway IP should be blank.

Remote LAN
Remote security gateway for which the security services should be provided. If the remote end is the host, this should be configured as **None**.

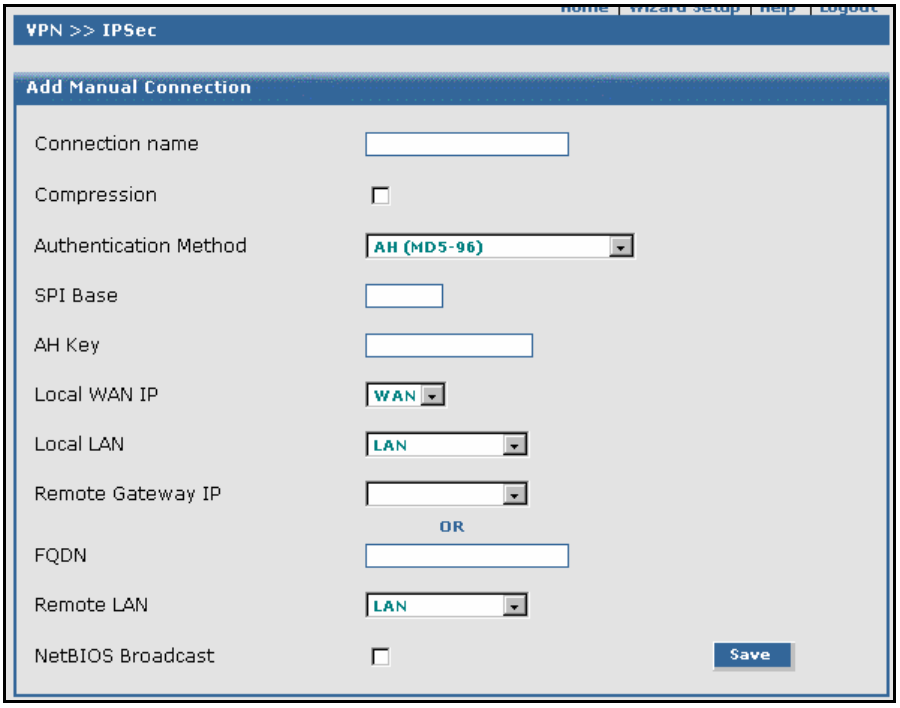
UID (Unique Identifier String)
It is recommended that you accept the default to disable UID. UID is used only for compatibility purposes (other IPSec VPN gateways might require you to input a Local and Remote IPSec Identifier). ***Note:*** Local ID and Remote ID are active only when UID is enabled for the connection.

Local ID
Enter the local security gateway ID, if required.

Remote ID
Enter the remote security gateway ID, if required.

NetBIOS Broadcast
Check this option to enable broadcasts over the connection. It will allow computers on the network to share Microsoft file and printer sharing information.

Add a Manual Connection



Add Manual Connection

Connection Name

Enter a text name that will identify the connection for you.

Compression

Check the compression checkbox to enable IPCOMP, the compression algorithm.

Authentication Method

Decides the encryption and authentication algorithms to be used for the respective security services. Options are:

Authentication only:
1. AH using MD5 –128 bit key
2. AH using SHA1 – 160 bit key

Encryption only:
1. ESP (Encapsulating Security Payload) using AES
2. ESP using DES – 56 bit key
3. ESP using 3DES – 192 bit key

Encryption & Authentication:
1. ESP using 3DES for encryption and MD5 for authentication
2. ESP using 3DES for encryption and SHA1 for authentication
3. ESP using 3DES for encryption and AH MD5 for authentication
4. ESP using 3DES for encryption and AH SHA1 for authentication

Note: Encryption without authentication is not recommended since it is not secure.

SPI Base

Security Parameter Index identifies a manual connection. The SPI is a unique identifier in the SA (Secure Association – a type of secure connection) that allows the receiving computer to select the SA under which a packet will be processed. The SPI Base is a number needed by the manual keying code. Enter any 3-digit hexadecimal number, which is unique for a security association. It should be in the form 0xhex (a number between 0x100 - 0xfff is recommended). If you have more than one manual connection, then the SPI Base must be different for each one.

ESP Encryption Key (Espenckey) - The VPN firewall box uses 3DES as its encryption algorithm. 3DES uses a 192 bit hexadecimal number as its encryption key.

ESP Authentication Key (Espauthkey) - The VPN firewall could use either MD5 or SHA1 for ESP authentication: MD5 - 128 bit key example: 0x01234567890123456789012345678901234567890ab.
SHA1 - 160 bit key example: 0x0123456789012345678901234567890123456789012345678901234567890

AH Key

The VPN firewall could use either MD5 or SHA1 for authentication
MD5 - 128 bit key example: 0x01234567890123456789012345678901234567890ab.
SHA1 - 160 bit key example: 0x0123456789012345678901234567890123456789012345678901234567890

Local WAN IP

Select the Interface to initiate the IPSec tunnel (Left Security Gateway). Options are LAN, WAN, and DMZ.

Local LAN

This is the local security gateway for which the security services are to be provided. If the RouteFinder acts as a host, this should be configured as **None**.

Remote Gateway IP

This is the interface in which the IPSec tunnel ends. In the case of a Road Warrior with a Dynamic IP address, this should be configured as **ANY**.

Remote LAN

This is the remote security gateway for which the security services are to be provided. If the remote end is a host, this should be configured as **None**.

NetBIOS Broadcast

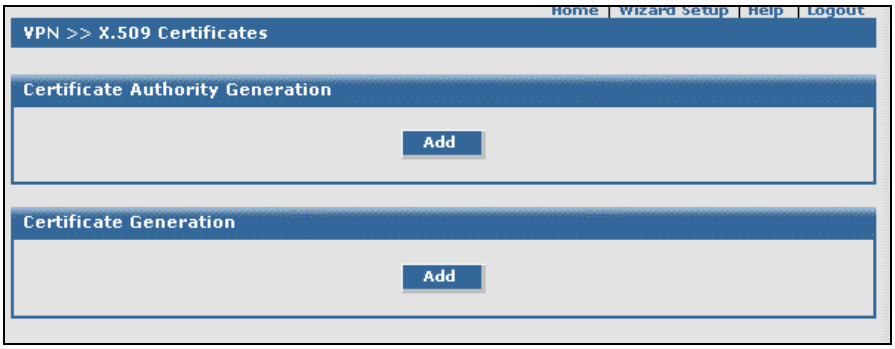
Check this option to enable broadcasts over the connection. It will allow computers on the network to share Microsoft file and printer sharing information.

VPN › x.509 Certificates

X.509 is an International Telecommunication ITU-T and ISO certificate format standard. The last release of this standard was X.509 Version 3 in the year 1996.

An X.509 certificate is a confirmation of identity by binding an entity's unique name to its public key through the use of a digital signature. It also contains the unique name of the certificate user. The certificate, issued by a certificate authority, contains information to protect data or to establish secure network connections.

When you click the **Add** buttons on this screen, secondary screens display.



Certificate of Authority Generation

A Certificate of Authority Generation screen opens when you click the **Add** button. On this screen, you can:

- Add a self-signed Certificate of Authority (CA) by entering the information necessary to identify your Certificate.
- Import a selected Certificate of Authority.
- Add a predefined Certificate of Authority.

Certificate Generation

A Certificate screen opens when you click the **Add** button. On this screen, you can enter the file path and key file path. Then enter your password and click **Import**. The certificate is then installed.

VPN › IPSec Bridging

IPSec Bridging is a concept by which two IPSec tunnels can be linked as if they form one single tunnel.

Example (In this example, there are two tunnels):

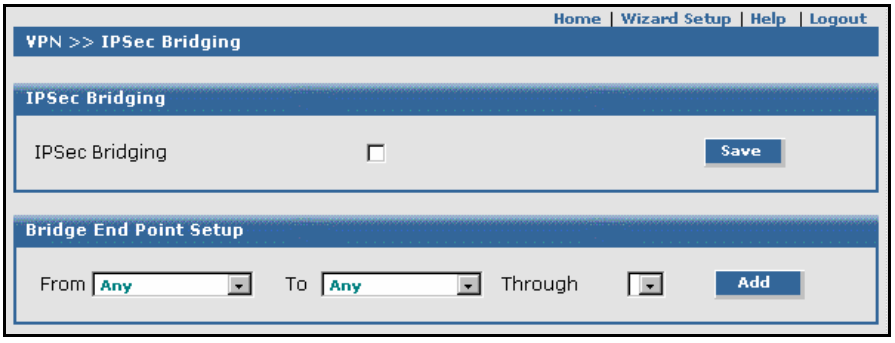
1. **tun1** between gateways **A** and **B** and
2. **tun2** between gateways **B** and **C**

If **A** and **C** have to communicate over a secure channel, then a third tunnel would have had to setup if IPSec Bridging was not used. But with IPSec Bridging, we can have them communicate through the existing tunnels, **tun1** and **tun2**.

The above concept can be extended to link more than two tunnels, provided they all have one common endpoint.

The common endpoint between tunnels is called a **hub**.

The other endpoints are called bridge **endpoints**.



IPSec Bridging

Check the box to enable IPSec Bridging. If enable IPSec Bridging, then this machine is going to act as a hub. Upon enabling IPSec Bridging, you will be given options to select the pairs of tunnels for which bridging is to be setup. See example above.

Bridge Endpoint Setup

Configure a tunnel and two networks by selecting the **From** network, the **To** network, and the **Through** tunnel. If any packet has a specified source and destination network, the packet will be sent encrypted via the tunnel.

Note: Packets are sent via the tunnels only if the tunnels are up and running.

VPN › PPTP

PPTP is a tunneling protocol meant for tunneling IP/non-IP packets through the IP only network (the Internet). The configuration of the VPN PPTP lets you grant single specified hosts access to your network via an encrypted tunnel. PPTP is considerably easier to set up than IPSec because, if Microsoft Windows is being used, it does not require additional software on the client computer as IPSec does. Also, PPTP is part of the Microsoft Windows program since Windows 95.

Notes:

- To be able to use PPTP with your RouteFinder, Windows 95 and 98 clients require a PPTP update from Microsoft at: http://support.microsoft.com/support/kb/articles/Q191/5/40.ASP.
- If you are using Windows or 98, you may also have to update Microsoft RAS update.

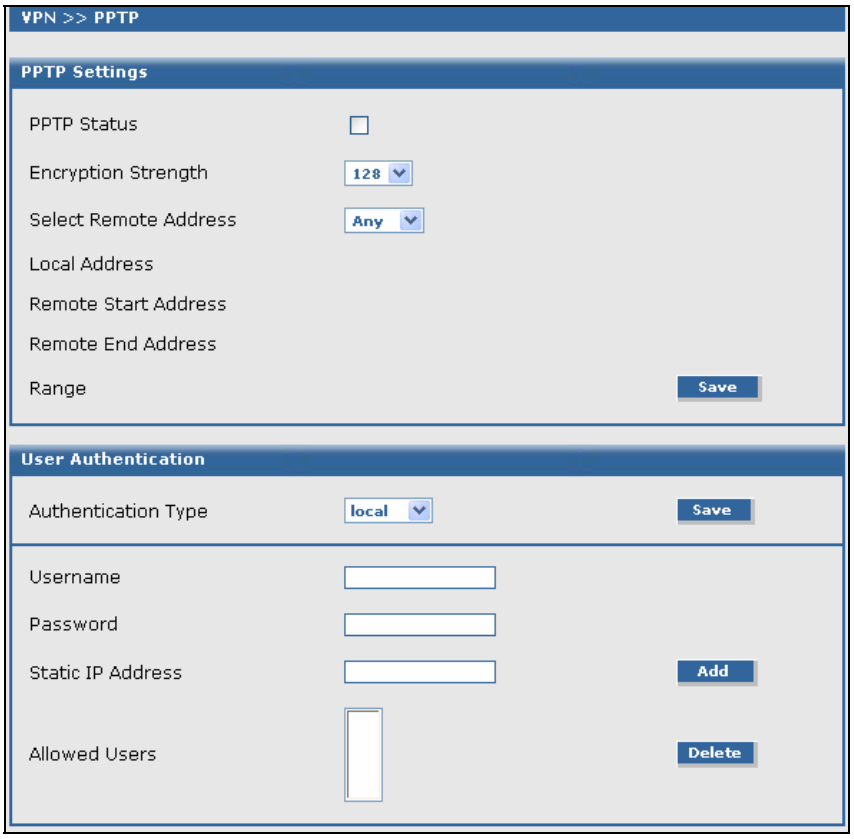
When enabling PPTP for the first time, a random network for use as a Pool will be generated. Clients will be given addresses from this network range.

About Setting Up PPTP Users

You can define your own pool and set it to be used as the PPTP pool. Alternatively, you can assign a special IP to each user when you define each user's account (see **Networks & Services**).

- This IP does NOT need to be from the pool.
- The client does not need to specifically request this IP address to be used. It will be assigned to the client automatically.

If an application such as online banking is not working after implementing the RouteFinder, you can see if any packets were filtered out and which rule was responsible for filtering them.



PPTP Settings

Status

Check the Status checkbox to enable this PPTP function.

Encryption Strength

Select the encryption strength, either strong (128 Bit, the default, or weak (40 Bit) encryption. This field defines the encryption strength (40 bit or 128 bit) for the remote access connection.

Notes:

Windows 98 and ME support strong encryption. Windows 2000 contains only 40-bit encryption strength. Windows 2000 users will need the High Encryption Pack or Service Pack 2 for strong encryption.

Select Remote Address

If you use private IP addresses for your PPTP pool, such as the predefined network, you must create Masquerading or NAT rules for the PPTP pool in order for the PPTP clients to be able to access the Internet. The network must be previously defined in the **Networks & Services > Networks**.

Select the Remote IP address for the PPTP link and click the **Save** button. Then the following fields display:

Local Address

Displays the local IP address of the server the remote clients will access.

Remote Start Address

Displays the first IP address in a range of IP addresses to be assigned to remote clients.

Remote End Address

Displays the last IP address in a range of IP addresses to be assigned to remote clients.

Range

Displays the total number of IP addresses that can be assigned to remote clients. The number of IP addresses available for use (e.g., 253).

User Authentication

Authentication Type

Select the type of authentication to be used. Options are Local or RADIUS. Click the **Save** button.

UserName and Password

Enter the name (in lowercase) and password (in lowercase) of the PPTP user. Click the **Add** button.

Allowed Users

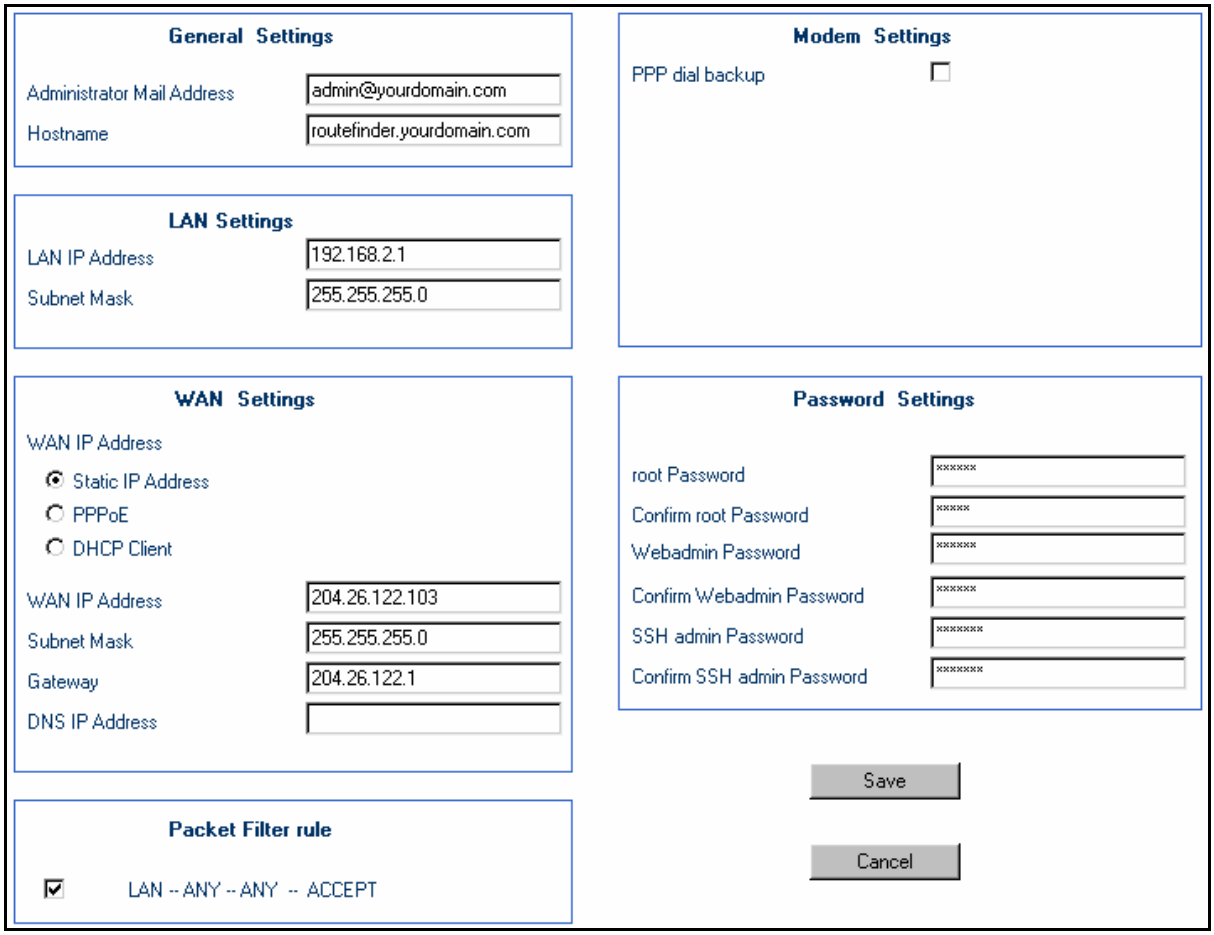
The names of the users entered above display in this text box. If you wish to delete a name, click the **Delete** button.

Wizard Setup

Using the Wizard Setup screen is a quick way to configure your RouteFinder. The screen contains the basic configuration input fields for setting up the RouteFinder as a firewall. If you desire to configure your RouteFinder to meet your company's specific needs beyond what is cover in the Wizard, use the Web Management software.

When you select Wizard Setup from the menu, a Java Security dialog box may or may not display. If a security dialog box displays, simply click the appropriate response to continue (i.e., **Yes**, **OK**, or **Grant This Session**).

Wizard Setup Screen



General Settings

Administrator Mail Address

Enter the administrator's mail ID. Unlike the Administration > System Setup in the Web Management software which allows several entries, the screen allows only one ID.
Host Name - Enter the Host Name of your firewall. Example format: FIREWALL.mydomain.com

LAN Settings

LAN IP Address and Subnet Mask

Enter the IP address and the mask for the LAN interface.

WAN Settings

Select the method of assignment of the IP address and mask for WAN interface. Choose one of the following:

Static IP Address

Click the Static IP Address button. Enter the IP address and mask for WAN interface. You can enter the gateway and DNS server addresses also.

PPPoE

Click the PPPoE button. The corresponding entry fields will display. Enter the ADSL User Name and Password provided by the ISP for the PPPoE connection.

DHCP Client

When selected, no other fields display.

Packet Filter Rule

If this setting is enabled by checking the checkbox, all packets coming from the LAN will be forwarded by the firewall. If disabled, none of the packets will go through.

Modem Settings

Use this checkbox to enable/disable the modem PPP dial backup feature. If enabled, enter the User Name, Password, Serial Port, Baud Rate, Dial Number, and Initialization Strings for the backup port.

Password Settings

Use this section to change the password for the root user, WebAdmin User, and the SSH User (login user). It is highly recommended that you change passwords.

Save or Cancel

When all of the parameters are set, click the **Save** button to activate them. Your RouteFinder is now configured.

Statistics & Logs

Various log files maintained by the RouteFinder can be viewed and/or downloaded to the browser. This function provides current system information, status, and usage information. The information is valuable for troubleshooting and for monitoring the RouteFinder's operational status and overall performance.
The following functions can be accessed under **Statistics & Logs**:

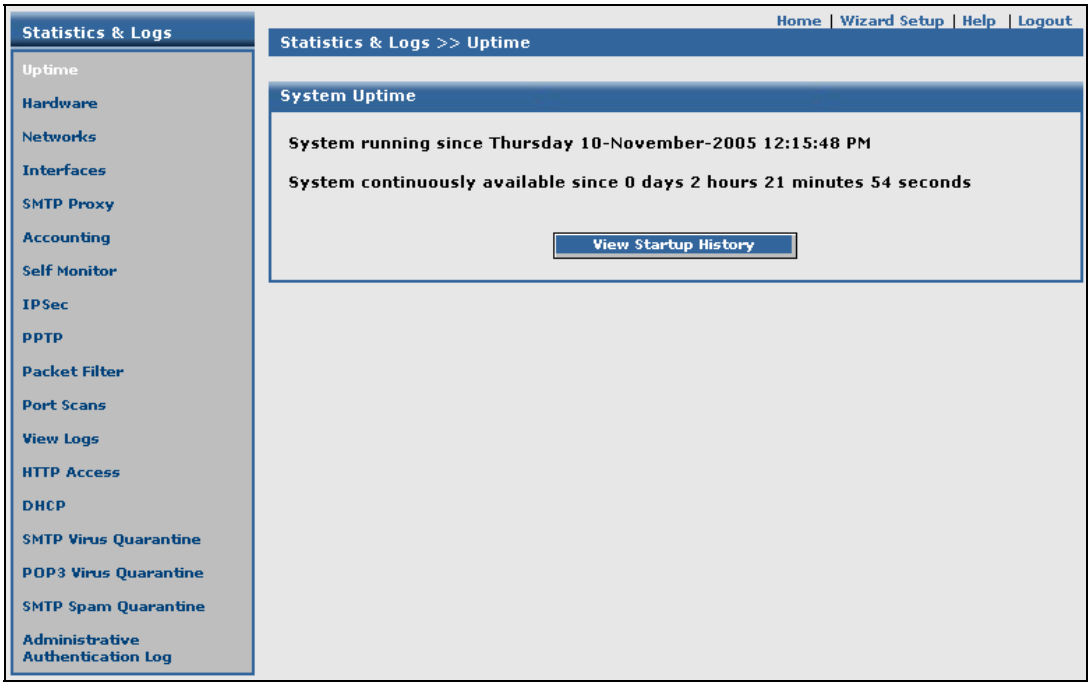
- Uptime (length of continuous RouteFinder operation and date last booted)
- Hardware (CPU, RAM, and Swap utilization)
- Networks (the internal network, NICs, Routing Table, and active Internet connections traffic)
- Interfaces (displays network traffic on each interface - LAN, WAN, DMZ)
- SMTP Proxy (displays email usage and status)
- Accounting (calculates and displays external NIC IP packet byte counts)
- Self Monitor (provides email notification of system-level issues)
- IPSec (displays VPN information)
- PPTP (displays processes and error messages)
- Packet Filters (displays defined filter rules, system-generated rules, and filter violations)
- Port scans (disables and logs attempted port scans)
- View Logs (displays a list of log files maintained by the RouteFinder
- HTTP Access (displays a list of users and the Internet sites visited by them)
- DHCP (displays information about the DHCP leases)
- SMTP Virus Quarantine (captures any virus-infected emails)
- POP3 Virus Quarantine (captures any virus-infected emails)
- SMTP SPAM Quarantine (using a Message Expression filter and an Attachment filter, SPAM emails will not be relayed and will be quarantined in the SPAM area. They can then be evaluated by the system administrator.
- Administrative Authentication Log (shows successful/failed login attempts)

The data in the logs could be useful to outside attackers, and it may well be considered confidential too. For security reasons, certain information should not be logged where an intruder could possibly access it.
The logs help you watch for usual patterns of usage, newly-developing trends in usage, and to alert you to any and all exceptions to these patterns of typical use. Administrators should become very familiar with the typical log patterns and messages, so that it can be recognized when something goes wrong (i.e., an unusual pattern of usage develops).
Generally speaking, log data falls into one of three categories:

1. ***Known to be OK -*** These are messages that can typically be ignored:
2. *System running since Monday 21 October-2002 02:30:44PM*, or *CNAME_lookup_failed_temporarily._(#4.4.3)/*, or *Watching superdaemon.pl ALL OK*.
3. ***Known to be problems -*** Messages that should cause some action (email the administrator, start investigating the cause, etc.). For example: a message about a bad disk block at location 0x56c8a7 or something similar.
4. ***Unknown -*** Messages that someone should examine, such as why someone is sending UDP packets from port 20 to some arbitrary port above port 1024 (doesn't match any known protocol).

Statistics & Logs › Uptime

Uptime tells you how long the system has been running. The first line displays the date and time the system was started. The second line displays the total time elapsed since the system was started in days, hours, minutes, and seconds.



Statistics and Logs › Hardware

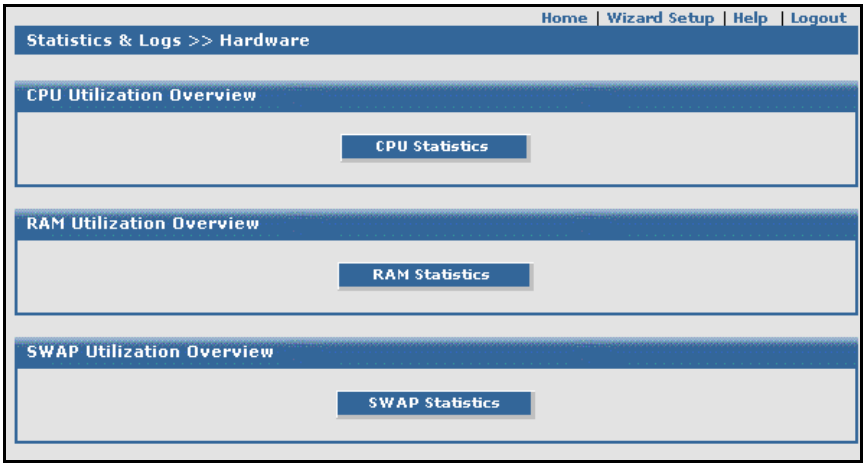
This screen displays a graphical presentation of the CPU, RAM, and SWAP utilization by days, weeks, months, and years.

CPU Statistics: Displays the actual usage of the processor on the system.

RAM Statistics: Displays the amount of RAM used by the various RouteFinder processes that are in execution.

SWAP Statistics: Shows the actual usage of the swap space on the system. When using the HTTP proxy is in use, frequent activity of the swap file is normal.

The log files are updated every five minutes and displayed in the **Hardware** charts.

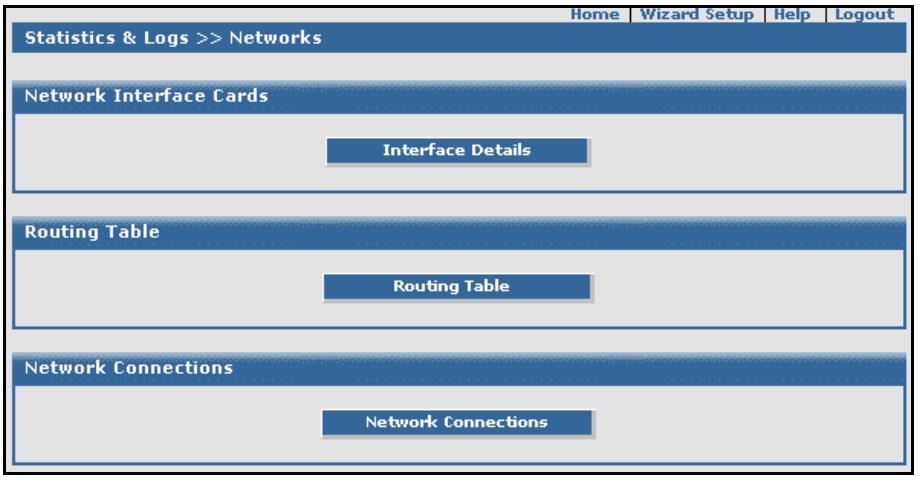


What the Graphs Show

The graph shows daily, weekly, monthly, and yearly **CPU**, **RAM** and **SWAP** utilization statistics.

Statistics and Logs › Networks

This menu displays an analysis of the RouteFinder network interface details, routing, and network connections.

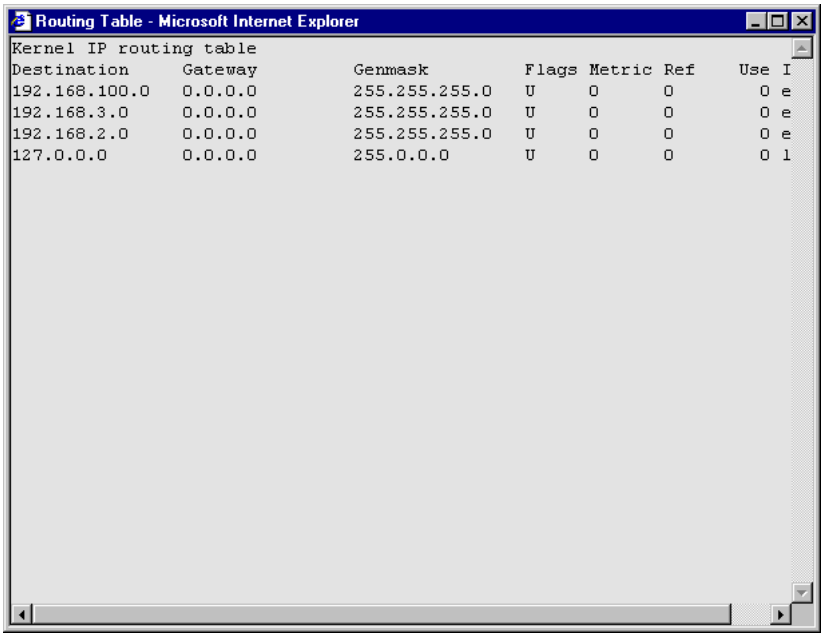


Network Interface Cards

Click the **Interface Details** button to display the Interface details about all the interfaces (Ethernet, IPSec, PPP, and local interfaces).

Routing Table

Click **Routing Table** to display the Kernel IP routing table of all entered routes. The information includes Destination, Gateway, Genmask, Flags, Metric, Ref(Reference), and Use, Iface (User Interface).
Important Note: Interface routes are inserted by the system and cannot be edited. Additional routes can be added in **Network Setup > Routes**. This is an example of the Statistics & Logs Routing Table report.



How to Read the Table

Destination

The address of the target system.

Gateway

The address of the next-hop router.

Use Iface (User Interface)

Indicates the name of the local interface from which the packet is to be sent.

Network Connections

Click the **Network Connections** button to display the status of all current (active) network connections to or from your RouteFinder. Information on the active protocol, receive queue, send queue, local address, foreign address, and current state is shown for each of the RouteFinder's active Internet connections. It also shows you all of the established TCP sessions and all of the TCP and UDP ports that the RouteFinder is listening to for incoming connections. (Connections through the RouteFinder are not shown).

TCP Connections Example

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State
tcp	0	0	0.0.0.0:22	0.0.0.0:*	LISTEN

This output tells you that your RouteFinder is listening (**LISTEN**) at all (**0.0.0.0**) interfaces for incoming requests to port 22 (ssh); the remote IP address is **ANY** (**0.0.0.0**) and the remote port does not care (the ***** in the **Foreign Address** column indicates **ANY**).

How to Read the Active Internet Connections part of the table

Proto

Protocol - TCP or UDP (RAW sockets are not supported).

Recv-Q

Receive Queue - An entry here means that the IP stack had received data at the moment you requested the output.

Send-Q

Send Queue - An entry here means that the IP stack had sent data at the moment you requested the output.

Local Address

Shows the local (Servers) IP address and the port separated by a colon (**:**). If you find here, for example, **192.168.2.43:443**, you know that there is an active HTTPS session.

Foreign Address

The destination IP address and port (for example **192.168.2.40:1034**).

State

Status of the connection – Sets of possible states reported are, for example:
LISTEN, ESTABLISHED. TIME_WAIT.

UNIX Connections Example

Proto	RefCnt	Flags	Type	State	PID Program name
UNIX	3	ACC	SOCK_STREAM	CONNECTED	609/syslog-ng

Proto

Protocol: UNIX

RefCnt

Reference Count – Attached processes via this socket.

Flags

Flags Displayed – Flags displayed are SO-ACCEPTON (displayed as ACC), SO_WAITDATA (W), or SO_NOSPACE (N). SO-ACCEPTON is used on unconnected sockets if their corresponding processes are waiting for a connect request. The other flags are not of normal interest.

Type

Shows types of socket access:
SOCK_DGRAM – The socket is used in Datagram (connectionless) mode.
SOCK_STREAM – This is a stream (connection) socket.
SOCK_RAW – The socket is used as a raw socket.
SOCK_RDM – This one serves reliably-delivered messages.
SOCK_SEQPACKET – This is a sequential packet socket.
SOCK_PACKET – Raw interface access socket.
UNKNOWN

State

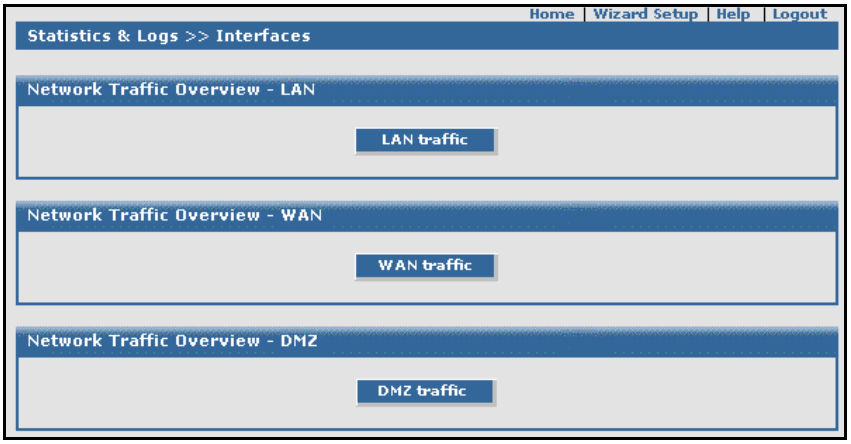
This field contains one of the following keywords:
FREE – The socket is not allocated.
LISTENING – The socket is listening for a connection request. Such sockets are only included in the output if you specify **- - listening (-l)** or **- -all (-a)** option.
CONNECTING – The socket is about to establish a connection.
CONNECTED – The socket is connected.
DISCONNECTING – The socket is disconnecting.
(empty) – The socket is not connected to another one.

PID/Program Name

Process ID (PID) and process name of the process that has the socket open.

Statistics & Logs › Interfaces

The information displayed under each option shows the network traffic on each interface (LAN, WAN, DMZ) delineated by days, weeks, months, and years. Interfaces must be added on the **Tracking > Accounting** screen.



Network Traffic Overview - LAN - WAN - DMZ

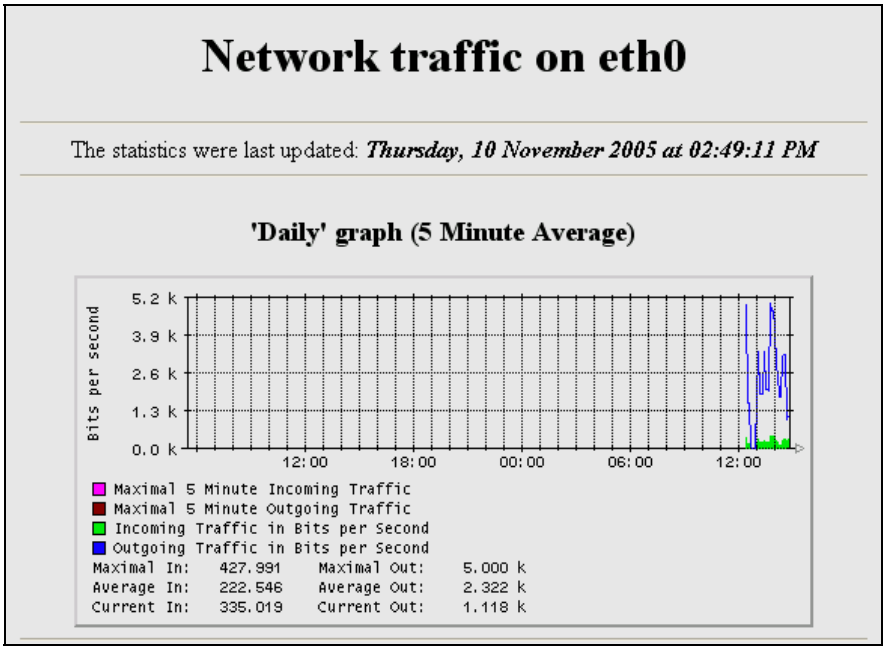
Click the **LAN Traffic** button for a graphical overview of network traffic on the LAN interface.

Click the **WAN Traffic** button for a graphical overview of network traffic on the WAN interface.

Click the **DMZ Traffic** button for a graphical overview of network traffic on the DMZ interface.

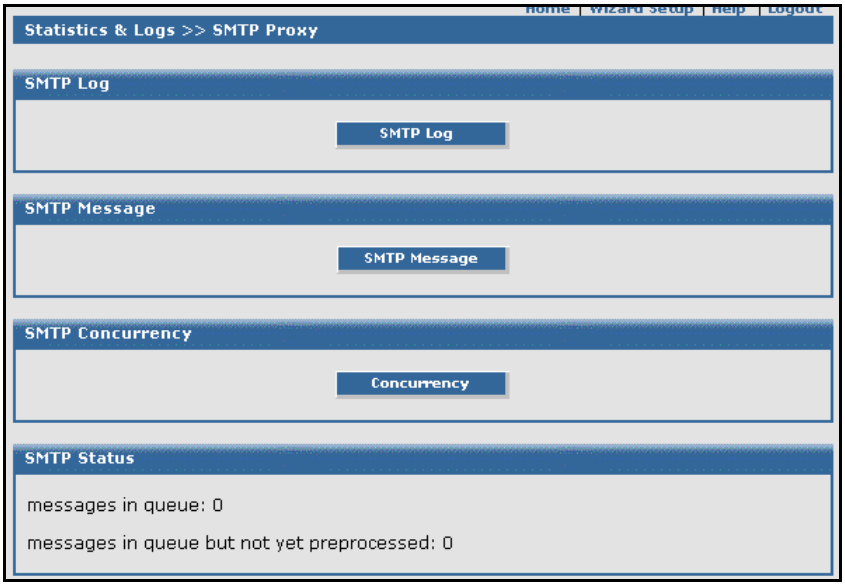
Example

Statistics are shown for daily, weekly, monthly, and yearly traffic. This example shows the daily graph for LAN traffic.



Statistics & Logs › SMTP Proxy

The **SMTP Proxy** screen displays the RouteFinder's SMTP proxy (email) usage and status in two windows called SMTP-Logs and SMTP-Status. It shows a real-time log of the email traffic via the SMTP proxy. The real-time log function is started by clicking the open SMTP Log button.



SMPT Log

Click the **SMPT Log** button to display real-time statistics of the SMTP proxy activities.

SMTP Message

Click the **SMTP Message** button to display a graph showing the number of messages in the queue waiting to be processed and the number of messages which are processed, separated by days, weeks, months, and years.

SMTP Concurrency

Click the **SMTP Concurrency** button to display the number of SMTP connections already established and the incoming and outgoing traffic in bytes per second, separated by days, weeks, months, and years. Shown as a graph.

SMTP Status

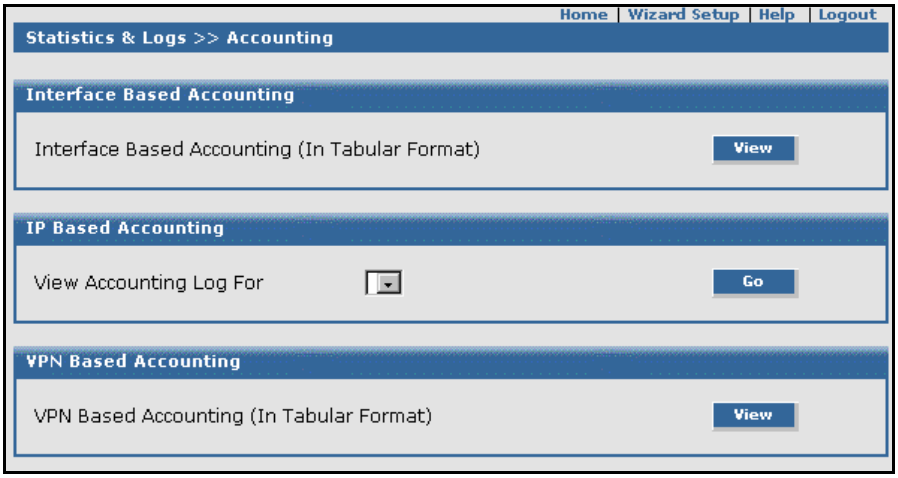
The SMTP Status displays the number of emails in the queue and the number of emails waiting to be processed.

Statistics & Logs › Accounting

This report gives the details of the amount of data transferred in bytes through the system on every interface (LAN, WAN, DMZ).

The **Accounting** function records all the IP packets on the external network cards and sums up their sizes. Each day's total is calculated once a day. Additionally, the number of bytes of data is calculated for each month.
The displayed traffic will match what your ISP charges if your service is volume-based.

Important: You define which interfaces and networks are included on this screen in the **Tracking > Accounting** menu.



Interface Based Accounting

Display accounting information for all the interfaces. Interfaces must be added on the **Tracking > Accounting** screen.

IP Based Accounting

Displays a graph of traffic from/to the selected IP address.

Note

If there are no entries in the drop down list box, you can add them on the **Tracking > Accounting** screen in the **IP-Based Accounting** section.

VPN Based Accounting

Displays the accounting information for all the IPSec tunnels that are currently enabled.

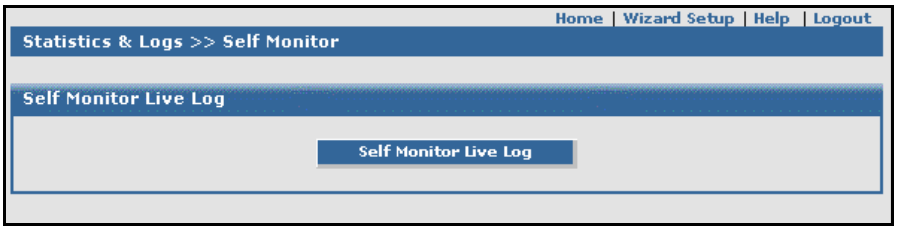
Statistics & Logs › Self Monitor

The **Self Monitoring** function ensures the integrity of the RouteFinder system and informs the administrator of important events by email. Self Monitoring controls the function, performance, and security of the system parameters and takes regulating measures when it detects divergences that go beyond a certain tolerance. The system administrator then receives a report via email.

Self Monitoring considerably reduces maintenance, as manual intervention becomes almost obsolete, resulting in less work for the administrator.

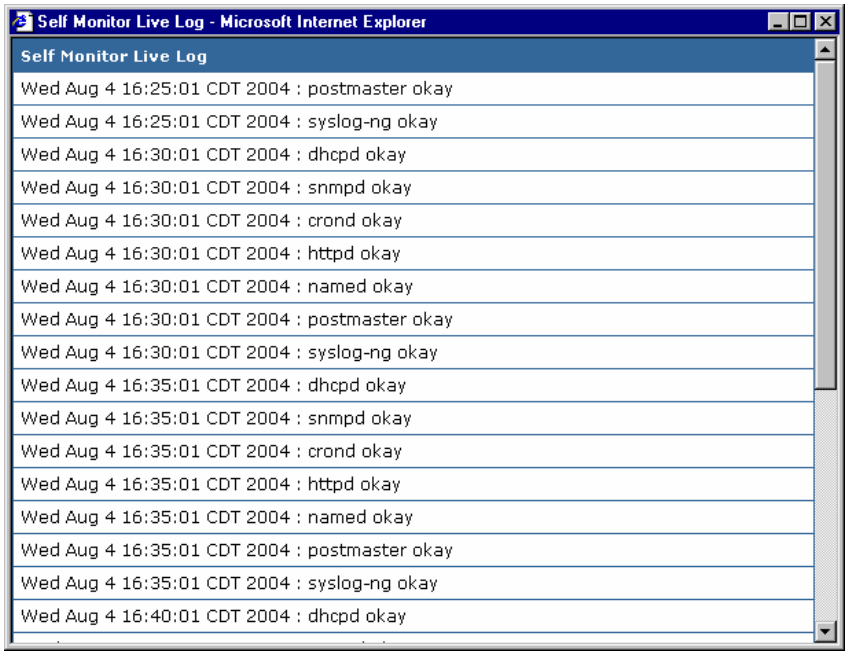
The RouteFinder's Self Monitoring function ensures that the central services (e.g., the RouteFinder MiddleWare daemon, the Syslog daemon, the HTTP proxy, or the network accounting daemon) function smoothly. The access rights to files are controlled, as is the individual process' share of consumption of the system resources. This prevents any possible RouteFinder overload. The administrator is also notified of any possible future resource shortage, such as a hard disk running low on space.

If no entries are displayed your RouteFinder is stable.

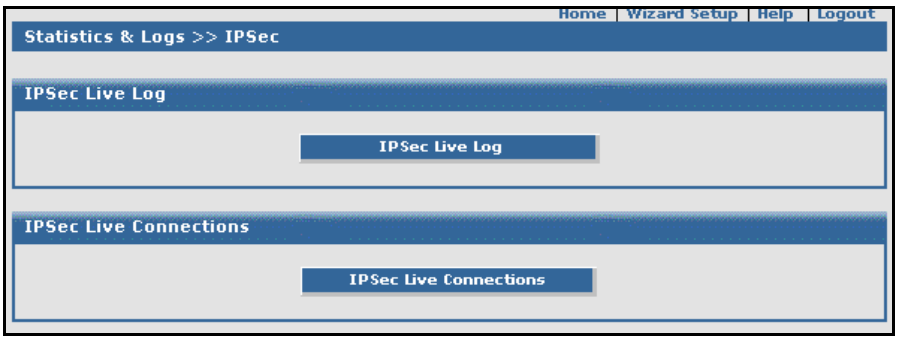


Click the **Self Monitor Live Log** button to open the report, which provides a record of the processes that have been restarted due to possible abnormal termination.

Example of a Self Monitor Live Log Report



Statistics & Logs › IPSec



IPSec Live Log

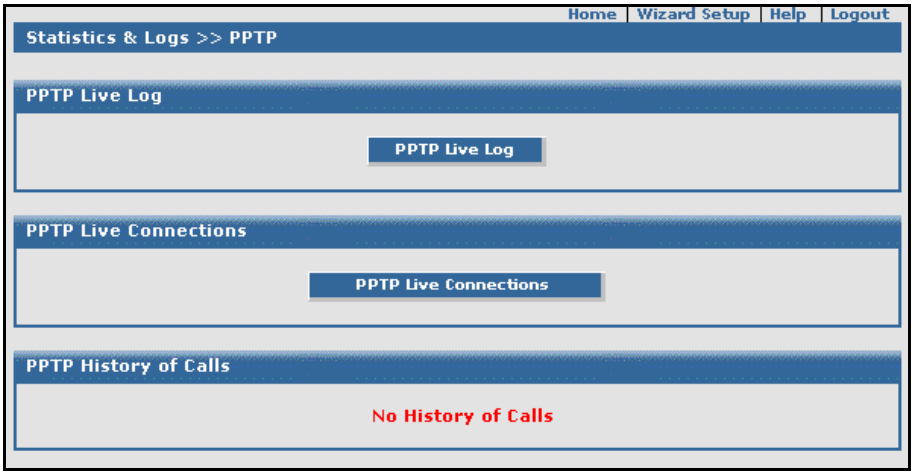
Click the **IPSec Live Log** button to display information about initialization, encryption/decryption messages, route manipulation, IPSec/IKE interaction, and IKE processing messages.

IPSec Live Connections

Click the **IPSec Live Connections** button to display realtime VPN statistics about active VPN routes and connections. It includes connection name, connect time, local gateway, remote gateway, security policy, tunnel end-point and important processes or error messages.

Statistics & Logs › PPTP

In the **PPTP LiveLog** you can view important processes or error messages. The logs provide you with the best chance of detecting attacks against your site, as well as for finding out the results of a successful attack. You will probably want to keep log information in a location separate from the RouteFinder, to keep an intruder from destroying the log data upon compromising the RouteFinder.



PPTP Live Log

Click **PPTP Live Log** button to display all the important information about PPTP logins (successful as well as failed), the encryption strength (128 or 40 bit), the mode of authentication (CHAP, MSCHAP, or MSCHAPv2), and user name.

PPTP Live Connections

Click the **PPTP Live Connections** button to display information about users who are logged into the server at any given point in time. This screen also displays information about the links on which the users are connected and the local and remote IP addresses of the links. It shows user name, connect date and time, and bytes received and sent.

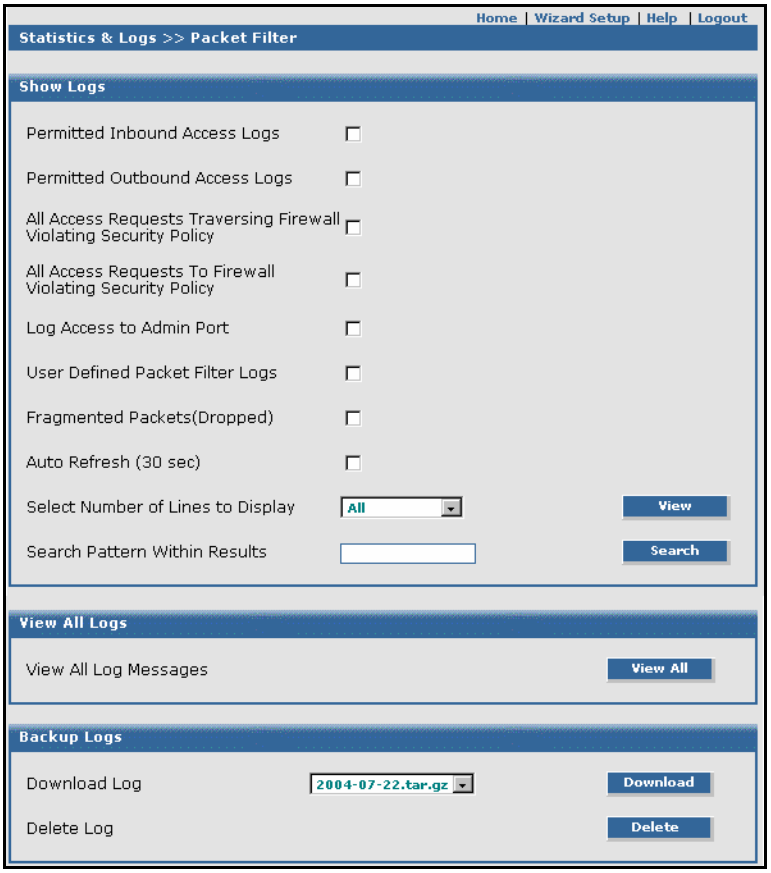
History of Calls

The **PPTP History of Calls** displays information about users who have connected so far. It shows connect date and time, user name, interface on which the user is connected, original IP address of the user, and total traffic transmitted and received.

Statistics & Logs › Packet Filter

This report shows the RouteFinder firewall logs for various types of packets. The type and number of packets to be displayed can be configured. You can also select the refresh rate of the log display.

In the **Packet Filter > Packet Filter Rules** page, if there is any user-defined filter with Action as LOG, the packets matching the corresponding source address and service will be logged.



Show Logs

Select the packets to be displayed by checking the box next to the packet category.

Check *Auto Refresh* if you like the screen to refresh every 30 seconds.

Select the number of lines from the log database to display on the screen.

Enter the *Search Pattern Within Results* – Enter the text pattern for which the system will search.

Click the **View** button to display the log file.

View All Logs

Select this option to view all logs listed above.

Backup Logs

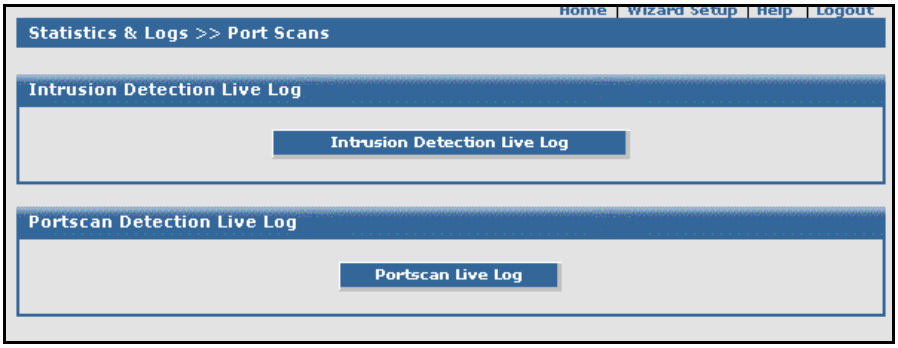
Use this section of the screen to backup your log files or to delete the current log files.

Statistics & Logs › Port Scans

The Port Scans screen displays the information gathered by the Network Intrusion Detection module, which guarantees the integrity of the system by watching and logging stealth port scans and suspicious packets. The system administrator will receive emails every hour if such packets are received.

You can setup User Defined Intrusion Detection rules on the **Administration > Intrusion Detection** screen.

Note: Apart from the use defined rules, the intrusion detection module will log port scans detected, but the destination address and port will not be displayed for these packets. Instead, the number of port scan attempts will be displayed.



Intrusion Detection Live Log

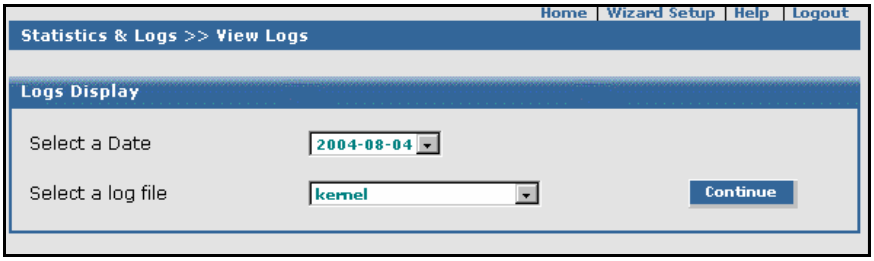
Click the **Intrusion Detection Live Log** button to display the **User Defined Intrusion Detection** rules entered on the **Administration > Intrusion Detection** screen.

Portscan Live Log

Click the **Portscan Live Log** button to display detected port scans. The source address, the destination address, protocol, source port, and destination port of these packets will be displayed.

Statistics & Logs › View Logs

Various log files maintained by the RouteFinder can be viewed and downloaded to the browser from this screen.
The other log file screens provide real-time view. This screen provides you with access to log files from previous dates. Logs available for viewing are Kernel Log, Daemon Log, HTTP Proxy Access, Network Intrusion Alert, IPSec, Self Monitor, URL Filtering, Mail Reply, PPP, PPTP, PPPoE, and SPAM Log.

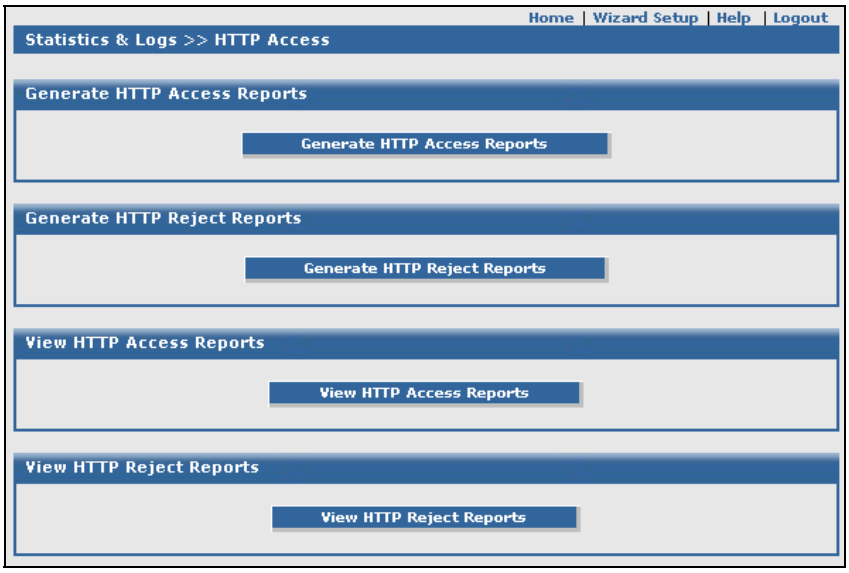


Logs Display - Select a Date and Select a Log File

1. First, select the date of the log file, and then select the type of log file.
2. Click the Continue button.
3. Another screen displays. On this screen, select the time and action to be taken. Actions may be:
   - Display the file
   - Search for a pattern in the file
   - Download the file
4. Click **Go**.

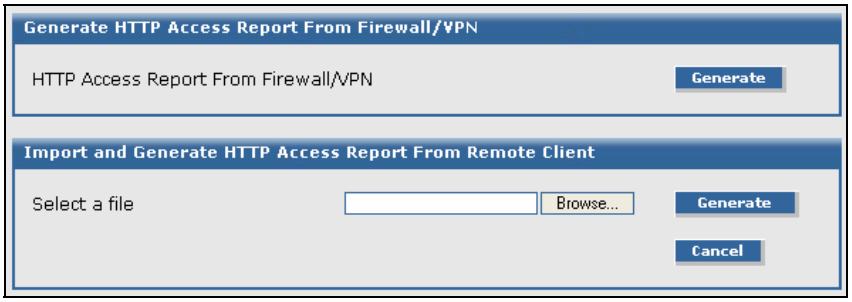
Statistics & Logs › HTTP Access

HTTP Access reports provide a clear picture of "where" your users are going to on the Internet.



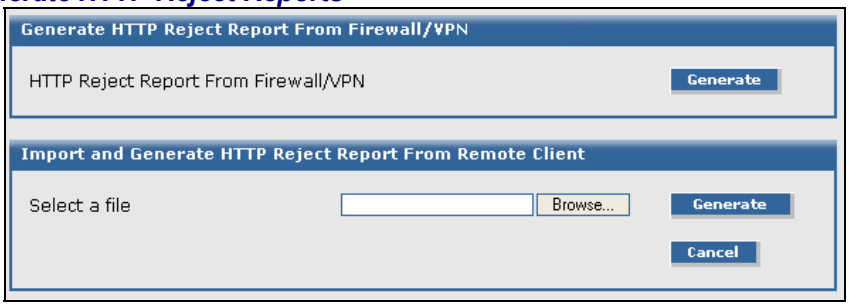
Generate HTTP Access Reports

This screen displays when the **Generate HTTP Access Reports** button is clicked (see screen above).



1. Click the **Generate** button to generate the current day's HTTP Access report.
2. Select a file from the remote client server by browsing to the file name and then clicking the **Generate** button. This will generate the HTTP Access Report from the Remote Client.

Generate HTTP Reject Reports



1. Click the **Generate** button to generate the current day's HTTP Reject report.
2. Select a file from the remote client server by browsing to the file name and then clicking the **Generate** button. This will generate the HTTP Reject Report from the Remote Client.

View HTTP Access Reports

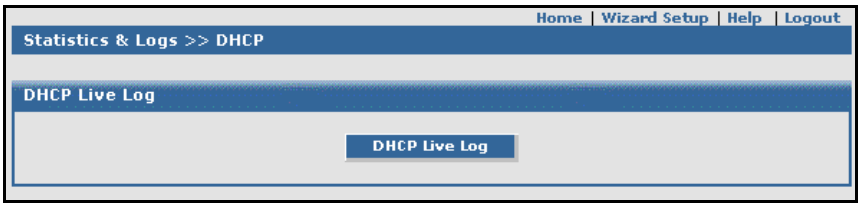
(See HTTP screen at top of the page) The report shows where users are going on the Internet. It includes the following information: Users, IP Address, bytes, sites, and times. You must enable **Status** and **Transparent** at **Proxy > HTTP Proxy**.

View HTTP Reject Reports

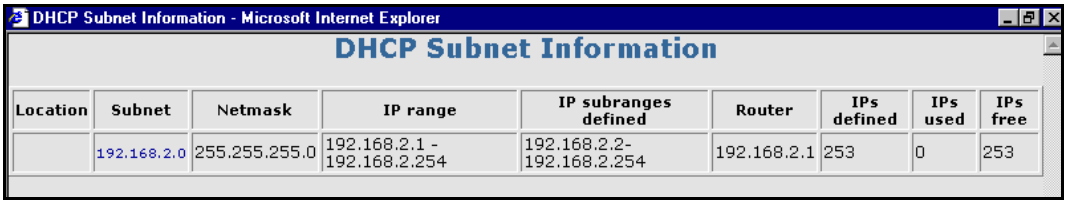
(See HTTP screen at top of the page) The report provides IP addresses / user names of the users who have tried to access denied sites. You must configure **Proxy > HTTP Proxy > URL Categorization** in order to view this report.

Statistics & Logs › DHCP

This live Log gives information about the DHCP leases that have been provided so far.



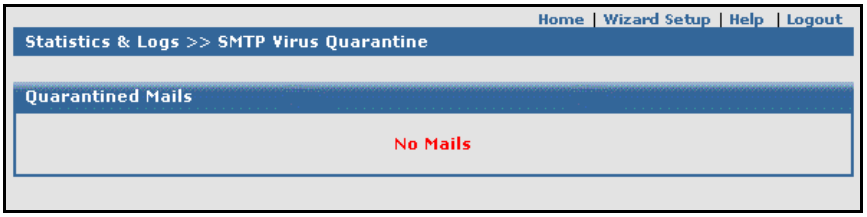
Example of a DHCP Log



Location	Subnet	Netmask	IP range	IP subranges defined	Router	IPs defined	IPs used	IPs free
	192.168.2.0	255.255.255.0	192.168.2.1 - 192.168.2.254	192.168.2.2- 192.168.2.254	192.168.2.1	253	0	253

Statistics & Logs › SMTP & POP3 Virus Quarantines

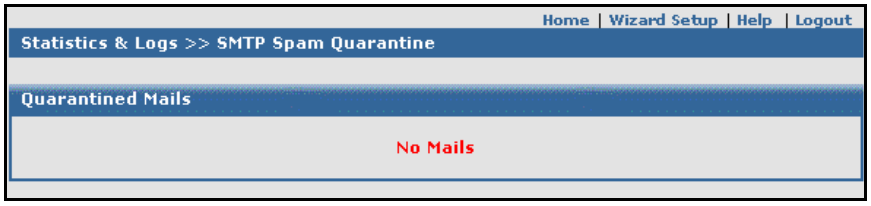
If the Virus Scanner is enabled, and if the SMTP proxy captures any virus infected emails, the emails will be saved in the virus quarantine area. These emails can be viewed by the administrator who can then take action as to whether or not to delete or forward the emails to the email ID.



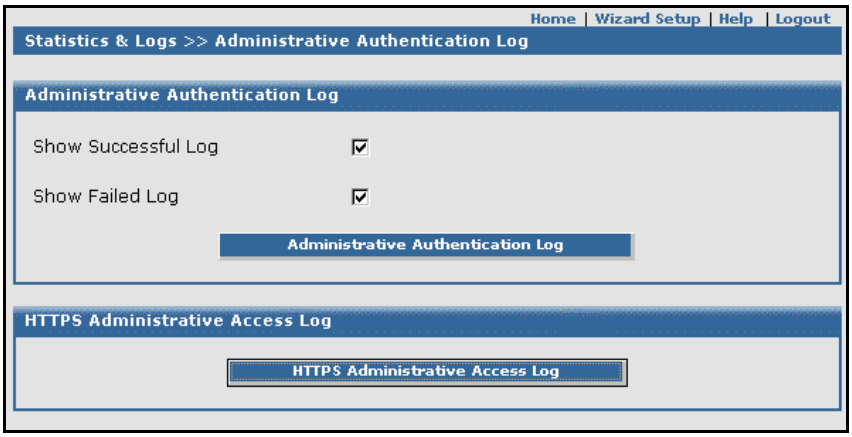
Statistics & Logs › SMTP SPAM Quarantines

If *Message Expression* filter or *Attachment Filtering* is enabled in **Proxy > SPAM Filtering**, and if such emails are to be relayed by the firewall, these emails will not be relayed and they will be saved in the SPAM quarantine area.

These emails can be viewed by the administrator who can then take action as to whether or not to delete or forward the emails to the email ID.



Statistics & Logs › Administrative Authentication Log



Administrative Authentication Log

Shows the successful and/or failed login attempts at the RouteFinder's Administrative Access interface. This log view is enabled on the **Administration > Administrative Access** screen.

HTTP Administrative Authentication Log

Shows all traffic that is directed at the RouteFinder's currently configured administrative HTTP access port. This log view is enabled on the **Administration > Administrative Access** screen.

Chapter 7 – User Authentication Methods

While you can restrict access of your internal clients to proxy services at the IP level by using packet filter rules, you will run into problems when you use a dynamic IP configuration protocol like DHCP or BOOTP internally. That's where Proxy User Authentication steps in. Here, clients must authenticate themselves to the proxy service with a username and password, making it possible to limit access by-person instead of by-IP address. In addition, it will also be possible to do "per-user" accounting, for example, in the HTTP proxy access logs.

Proxy Services and Authentication Methods

The RouteFinder currently includes two proxy applications: SOCKS5 and HTTP. Both of these proxies can be configured to accept all clients (access control based on IP addresses) or only clients providing a valid username and password (User Authentication). If you select to use User Authentication for either of these proxy services, you must select a method for the RouteFinder to validate the supplied credentials. The RouteFinder currently supports User Authentication against:

- A RADIUS server configured in **Administration > User Authentication > Radius & SAM**
- An NT SAM User Base configured in **Administration > User Authentication > Radius & SAM**
- Users defined in **Administration > User Authentication > Local**

RADIUS User Authentication

With this method ASL will forward User Information to a RADIUS server. RADIUS is a protocol typically used to authenticate and account Dialup Users for Remote Access. However the protocol is very flexible and RADIUS servers are available for almost every operating system including Microsoft Windows NT and 2000.
The RouteFinder's implementation of the RADIUS method allows you to configure access rights on both a per-proxy and a per-user basis.

NT SAM (SMB) User Authentication

This method uses a Microsoft Windows NT/2000 domain controller to validate user accounts. Many companies already run NT/2000 networks based on Microsoft NT or Windows 2000 Active Directory Domain concepts. The advantage of this method is that it is very easy to set up if you already run a PDC (Primary Domain Controller) on your network. The disadvantage is that only a "flat" authentication model is supported, meaning that either ALL or NONE of the existing users in the NT Domain will be allowed to use a proxy service (meaning that you cannot differentiate between User A and User B).

"Local" RouteFinder User Authentication

This method does not need an external server to validate user accounts. You can add users with the RouteFinder's Web front end and specify the allowed proxy types on a "per-user" basis.

Which Method Should You Choose?

This section provides possible scenarios that can help you decide which method of user authentication is the right one for your implementation of the RouteFinder.

Scenario 1: "Just a couple of Windows boxes"
You are running a small peer-to-peer network without a domain controller or other centralized authentication. This will typically be a SOHO or "family home" network.

- You should use "Local" ASL user authentication.

Scenario 2: "Microsoft-style Windows Network with all valid users able to use proxy services"
You are running a Windows Domain controller or a standalone server on your network, holding User Accounts. Typically, this is also the case if you are running MS Exchange on your network and you want every valid user to be able to use the proxy services.

- You should use NT SAM (SMB) user authentication.

Scenario 3: "Microsoft-style Windows Network - not all valid users able to use proxy services"
You are running a Windows Domain controller or a standalone server on your network holding User Accounts. Typically, this is also the case if you are running MS Exchange on your network, but not all of your users should be able to use proxy services.

- You should use RADIUS user authentication with Microsoft's IAS (Internet Authentication Server).

Scenario 4: "Unix or Netware Network"
You are running any other type of Network with a centralized user base.

- In this case, you can use RADIUS user authentication; however, it is up to you to find a suitable RADIUS server for your network type.
- You can also use the "Local" user authentication, but you must re-define all your users in the RouteFinder Web Front end.

Note: Many mixed scenarios are also possible. For example, you could have some local users being able to use the SOCKS service, plus a RADIUS server authenticating users for the HTTP proxy service.

Authentication Setup

Choose one of the following setup methods.

Setting Up RADIUS Authentication

To set up RADIUS Authentication, first you need a RADIUS server on your network. The server can be anywhere on the Internet, but keep in mind that passwords are transferred in clear text. Therefore, we strongly recommend putting the RADIUS server somewhere near your RouteFinder and to use a switched Network hub to connect them.
Choosing the RADIUS server is up to you. Below is some generic setup information.
The RouteFinder will send a RADIUS authentication packet with three fields:

1. Username
2. Password in plain text (PAP)
3. The proxy type ("http" or "socks") in the NAS-Identifier field based on these values, your RADIUS server should just decide to grant or deny access.

Setting Up A Microsoft IAS RADIUS Server

This section explains how to set up a Microsoft IAS (Internet Authentication Server). IAS is delivered with all Windows 2000 Server versions. However, it is often not installed by default. For NT4, IAS comes with the "NT4 Option Pack" (available for "free"). The Windows 2000 IAS version has many more features than NT4 IAS; however, the NT4 version is also sufficient for a typical RouteFinder authentication setup. Below are some generic IAS step-by-step instructions.

1. Check if the IAS service is installed. If not, install it.
2. Using NT/2000 **User Manager**, edit the user profiles of all Users who should use proxy services, and set the "Dial-In Permission" flag. This is necessary since IAS uses the "master flag" to respond to requests positively.
3. Create a new user group for each proxy service you wish to provide to your users. For clarity, give the groups descriptive names (for example, call the group "multitech _http_users").
4. Put the users in the newly created groups for using the respective proxy services.
5. Enter the IAS administration interface at (**Start->Programs->Administrative Tools->Internet Authentication Service**), and add a new client using these settings:

   Friendly Name: **routefinder**
   Protocol: **RADIUS**
   Client Address: Use the address of the RouteFinder's interface pointing "towards" the RADIUS server (this will be the "internal" interface for most people).
   Client Vendor: **RADIUS Standard**
   Uncheck the **Client must always send signature attribute ...** box.
   Select a shared secret. You will need this later in RouteFinder configuration.

6. Go to the policy list. There is one pre-defined entry. Delete it. Add a new Policy for each proxy service you wish to provide to your users. Choose the "Friendly Name" accordingly ("SOCKS access" for example).
7. On the next screen, add two conditions:
   - NAS-Identifier matches <string> (where <string> is the proxy identifier, currently "socks" or "http")
   - **Windows-Groups matches <yourgroup>** (where <yourgroup> is one of the newly created user groups).

   Note: You can add groups from the local machine or from Domains in which the RADIUS server is a member. User may have to specify the user name as <DOMAIN>\<USER> for authentication to succeed.
8. Choose **Grant Remote Access Permission** in the next screen.
9. Edit the profile on the next screen. Select the Authentication Tab. Check Unencrypted Authentication (PAP).
10. Click **OK** and **Finish**. Remember you need one policy for each proxy service.
11. Configure the RADIUS authentication method on the RouteFinder (you will need the IP of the IAS server and the shared secret), and use the **RADIUS** authentication method in **User Authentication > RADIUS & SAM** settings.
12. Check the System Log in the NT/2000 Event Viewer; that's where NT/2000 puts information about RADIUS authentication requests.

Setting Up NT/2000 SAM (SMB) Authentication

To setup Windows NT/2000 SAM Authentication, you will need an NT/2000 machine on your network that holds the user accounts. This can be a domain controller (PDC) or a simple standalone server. The server has a NETBIOS name (the NT/2000 server name) and an IP address.

Put these values in the configuration of the NT SAM method in **User Authentication > RADIUS & SAM** as PDC Name and PDC address. If you have a Backup domain controller, also enter its corresponding values in **User Authentication > RADIUS & SAM**.

Finally, you need the default domain to authenticate against. This will be overridden if users specify their user name as **<DOMAIN>\<USERNAME>**. Otherwise, it will be filled in as the **<DOMAIN>** part.

Caution: Disable the **Guest** account of your NT domain, since this one will allow **Any** username/password combination to pass!

Chapter 8 – Frequently Asked Questions (FAQs)

Q1. In general, what does the RouteFinder do?
A1. The RouteFinder VPN Gateway/Firewall Router lets you use data encryption and the Internet to securely connect to your telecommuters, remote offices, customers, or suppliers while avoiding the cost of expensive private leased lines. The browser-based interface eases VPN configuration and management. The VPN functionality is based on the IPSec and PPTP protocols and uses Triple DES 168-bit encryption to ensure that your information remains private. In addition, the RouteFinder includes firewall security utilizing Stateful Packet Inspection and Network Address Translation.

Q2. What is VPN and how do I use it?
A2. VPN (Virtual Private Networking) uses IPSec and PPTP industry standard protocols, data encryption and the Internet to provide high-performance, secure communications between sites without incurring the high expense of leased lines. The RouteFinder can connect individual telecommuters to the office network by creating a separate, secure tunnel for each connection, or it can connect entire remote office networks together as a LAN-to-LAN connection over the Internet using a single data tunnel.

Q3. Where is the RouteFinder installed on the network?
A3. In a typical environment, the RouteFinder is installed between the internal network and an external network. Refer to Chapter 1 and 2 of this manual for more information.

Q4. What is Network Address Translation and what is it used for?
A4. Network Address Translation (NAT) translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet. Furthermore, NAT allows the RouteFinder to be used with low cost Internet accounts, such as DSL or cable modems, where only one TCP/IP address is provided by the ISP. The user may have many private addresses behind this single address provided by the ISP.

Q5. What is a "DMZ"?
A5. The DMZ (Demilitarized Zone) is a partially protected area where you can install public services. A device in the DMZ should not be fully trusted, and should only be used for a single purpose (such as a web server, or an FTP server).

Q6. If DMZ is used, does the exposed user share the public IP with the Router?
A6. Yes.

Q7. What is the maximum number of users supported by the Router?
A7. Shared broadband or dedicated Internet access for up to 253 LAN users with one IP address. The RouteFinder supports up to 50 IPSec or 50 PPTP tunnels on the RF660/760VPN and 25 tunnels on the RF600VPN for secure LAN-to-LAN and Client-to-LAN access over the Internet.

Q8. Does the RouteFinder support virus protection?
A8. Yes - The optional virus protection subscription utilizes a high-performance, ICSA-tested, anti-virus engine which checks both incoming and outgoing email for viruses in real-time. With this option, automatic anti-virus updates will be downloaded at user-defined intervals.

Q9. What about RouteFinder firewall security support?
A9. As small businesses shift from dial-up to always-on broadband Internet connections or leased line connections, their networks become more vulnerable to Internet hackers. The RouteFinder uses Stateful Packet Inspection technology and the NAT protocol to provide security from hackers attempting to access the office LAN. An automatic update feature provides the highest level of security by automatically downloading any new system updates protecting against newly discovered hacker threats. Additionally, the RouteFinder uses proxies to filter Internet content protecting against dangerous ActiveX controls or Javascript and unwanted Web content.

Q10. Is Virtual Server support provided on my RouteFinder?
A10. Yes, in addition to providing shared Internet access, the RouteFinder can support a Web, FTP, or other Internet servers. Once configured, the RouteFinder only accepts unsolicited IP packets addressed to the web or ftp server. Refer to Chapter 3.

Q11. Is it possible to define a static NAT from the outside to the inside, (e.g., Map external IP a.b.c.d to internal IP w.x.y.z) in both directions?

A11. Yes, it is possible to do static NAT, but with limitations:

You can map:	You cannot map:
IP/Port => IP/Port	IP => IP
IP/Port-Range => IP/Port	IP-Range => IP
IP-Range/Port => IP/Port	IP => IP-Range (load balancing)
IP-Range/Port-Range => IP/Port	

The way back is done automatically.

NAT is done before the packets pass the packet filter, so you also have to make a rule allowing these IP-Packets to pass. There are 4 dropdown boxes in **Network Setup > SNAT**. The first two define which IP-Packets will be translated. The second two define into which IP/Port address they are translated.

Example:

Net1: 212.5.63.4/255.255.255.255 (Box1)
Srv1: 0:65535 TCP 80 (Box2)
Net2: 192.168.100.2/255.255.255.255 (Box3)
Srv2: 0:65535 TCP 81 (Box4)

Explanation:

If an IP-Packet from a.b.c.d port 34232 is sent to 212.5.63.4 port 80 (www) [a.b.c.d:34232 -> 212.5.63.4:80] and it reaches the RouteFinder, the destination information will be translated into [a.b.c.d:34232 -> 192.168.100.2:81]. If NAT is done before reaching the packet filter, you have to set the packet filter rules correctly.

Q12. Is it possible to have multiple IPs assigned to the external interface, and then have multiple internal Web-servers?

A12. Yes that is possible. You have to be sure that the request reaches the RouteFinder, and then you can use DNAT to redirect them to the Web servers. You don't need to bind those IP addresses to the external interface, as long as they are routed to the RouteFinder. The problem is that the IP packets have to reach the interface. There are 2 ways to accomplish this:

1. Bind an alias IP to the external interface, so that it answers ARP requests for this IP and the IP packets are sent to the ARP Address of this NIC card.
   (If you're ready to do some hand typing on the console you can make an IP alias on your NIC and make a script in /etc/rc.d/rc2.d to have it run at each boot (put it at S99 to be sure). Just don't use ***ifconfig*** to do that, as it is deprecated in 2.4 kernels.
   The command to add the IP 10.0.0.3 on your **eth0** NIC card is:
   IP addr add 10.0.0.3/24 broadcast 10.0.0.255 label eth0:0 dev eth0
   Note that the label part is not mandatory; it's just there so that ifconfig can list your alias. Moreover, the label name is free (you can have 'myalias' instead of eth0:0) though you should avoid characters like '-' or '_' : ifconfig seems to get lost if you use these.)
2. Tell the RouteFinder to send those IP packets directly to the external interface by adding a static routing entry. You have to do subnetworking; for example, enter the following interface definitions and routes:

OLD:	**NEW:**
RouteFinder: Router Ethernet Interface: IP: 196.126.228.65 Netmask: 255.255.255.224 Routes: none Firewall: RouteFinder Ethernet Interface: IP: 196.126.228.66 Netmask: 255.255.255.224 Def GW: 196.126.228.65	RouteFinder: Router Ethernet Interface: IP: 196.126.228.65 Netmask: 255.255.255.252 Routes: 196.126.228.67/255.255.255.252 -> 196.126.228.66 196.126.228.72/255.255.255.248 -> 196.126.228.66 196.126.228.80/255.255.255.240 -> 196.126.228.66 RouteFinder Ethernet Interface: IP: 196.126.228.66 Netmask: 255.255.255.252 Def GW: 196.126.228.65

Q13. Can I forward SSH connections?

A13. Yes, by configuring port forwarding of SSH (dest. port 22):
Source: External Interface Port 22 goes to
Destination: SSH_Server Port 22
Procedure:

1. Define two Hosts in **Networks & Services**:
   external_NIC a.b.c.d 255.255.255.255
   SSH_Server e.f.g.h 255.255.255.255
2. Define one Service in **Networks & Services**:
   NAT_SSH TCP 0:65534 22
3. Add one NAT-Rule in **Network Setup > DNAT**: external_NIC NAT_SSH -> SSH_Server NAT_SSH.
4. Add one Rule in **Packet Filters > Packet Filter Rules**: Any NAT_SSH SSH_Server Allow.

This way, the destination address of every TCP packet will be translated from a.b.c.d:22 (Firewall) to e.f.g.h:22 (SSH-Server) and back again.

Q14. SNAT: what is it and what would I use it for?

A14. SNAT is similar to Masquerading.
Definition SNAT (DSNAT): With SNAT you can rewrite the original Source Address of a specific IP connection with another static IP address.
You must make sure that the answer comes back to the firewall (e.g., if you want to access a Cisco router via telnet and the RouteFinder only allows connects from a specific static IP address, you can specify this in Source NAT.
Define a rule like: AdminPC, Telnet, Cisco Router > Allowed Cisco IP.
Now you can communicate with the Router. This is needed for more complex configurations.

Q15. How do I set up RouteFinder Masquerading?

A15. Configure Masquerading in WebAdmin:

1. Define Interfaces in **Network Setup > Interface**. Here you define your Network Interface settings as well as your default gateway, for example:
   LAN Internal: 192.168.100.1/255.255.255.255
   WAN External: 194.162.134.10/255.255.255.128
   Gateway: 194.162.134.1/255.255.255.128
2. Define Network definitions in **Networks & Services > Networks**. Here you define your host and network definitions, which you will use for further configuration like Masquerading or Packet Filter Rules later on (i.e., Internal-Network 192.168.100.0 255.255.255.0 / Peters-Laptop 192.168.100.12 255.255.255.255).
3. Define Masquerading in **Network Setup > Masquerading**. Here you define which network should be masqueraded on which network interface (i.e., **Internal-Network > External**).
4. Define Packet filter Rules and Proxy Settings. Now you have set your Security Policy in terms of what is allowed and what is not allowed. The RouteFinder uses stateful inspection, so you only have to define which services are allowed; the way back is opened automatically (e.g., **Internal-Network - FTP - Any - Accept | Peters-Laptop - Telnet - Any - Accept**). If you want to use the Proxies you can configure them in **Proxy**.

Q16. Can I do DNAT with Port ranges?

A16. Yes. Mapping DNAT port ranges is supported, with the limitation that you can only map the same range (so, for example, you can map ports 500-600 to 500-600 but not 500-600 to 300-400).

Q17. Does NAT take place before or after routing and filtering take place?

A17. In short, DNAT is done before the packets pass the packet filter, and SNAT and Masquerading are done after that. The RouteFinder uses a 2.4 kernel and IP tables (the internal logic in the netfilter code).

Q18. What are the current Certificate export laws?

A18. New US encryption export regulations took effect on January 14th, 2000. At the time of this publication, CAs may export certificates to any non-government entity and to any commercial government-owned entity (except those that produce munitions), in any country except Afghanistan (Taliban-controlled areas), Cuba, Iran, Iraq, Libya, North Korea, Serbia (except Kosovo), Sudan and Syria.
For the latest information on United States cryptography export and import laws, contact the Bureau of Export Administration (BXA) (http://www.bxa.doc.gov/).
For many years, the U.S. government did not approve export of cryptographic products unless the key size was strictly limited. For this reason, cryptographic products were divided into two classes: products with "strong" cryptography and products with "weak" (that is, exportable) cryptography. Weak cryptography generally means a key size of at most 56 bits in symmetric algorithms. Note that 56-bit DES keys have been cracked. In January 2000 the restrictions on export regulations were dramatically relaxed. Today, any cryptographic product is exportable under a license exception (i.e., without a license) unless the end-users are foreign governments or embargoed destinations (Cuba, Iran, Iraq, Libya, North Korea, Serbia, Sudan, Syria, and Taleban-controlled areas of Afghanistan, as of January 2000). Export to government end-users may also be approved, but under a license.

Q19. Why is the export of cryptography controlled?

A19. Cryptography is export-controlled for several reasons. Strong cryptography can be used for criminal purposes or even as a weapon of war. In wartime, the ability to intercept and decipher enemy communications is crucial. Therefore, cryptographic technologies are subject to export controls. U.S. government agencies consider strong encryption to be systems that use key sizes over 512 bits or symmetric algorithms (such as triple-DES) with key sizes over 56 bits. Since government encryption policy is influenced by the agencies responsible for gathering domestic and international intelligence (e.g., the FBI and NSA), the government tries to balance the conflicting requirements of making strong cryptography available for commercial purposes while still making it possible for those agencies to break the codes, if need be.

To most cryptographers, this level of cryptography (56 bits for symmetric algorithms) is not necessarily considered "strong". Government agencies use the terms "strategic" and "standard" to differentiate encryption systems. "Standard" refers to algorithms that have been drafted and selected as a federal standard (DES being the prime example). The US government defines "strategic" as any algorithm that requires "excessive work factors" to successfully attack. Unfortunately, the government does not frequently publish criteria for what it defines as "acceptable" or "excessive" work factors.

Q20. Can digital signature applications be exported from the U. S.?

A20. Digital signature applications are one of the nine special categories of cryptography that automatically fall under the more relaxed Commerce regulations; digital signature implementations using RSA key sizes in excess of 512 bits were exportable even before the year 2000. However, there were some restrictions in developing a digital signature application using a reversible algorithm (that is, the signing operation is sort of the reverse operation for encryption), such as RSA. In this case, the application should sign a hash of the message, not the message itself. Otherwise, the message had to be transmitted with the signature appended. If the message was not transmitted with the signature, the NSA considered this quasi-encryption and the State controls would apply.

Q21. Can DES be exported from the U.S. to other countries?

A21. For years, the government rarely approved the export of DES for use outside of the financial sector or by foreign subsidiaries of U.S. companies. Several years ago, export policy was changed to allow the unrestricted export of DES to companies that demonstrate plans to implement key recovery systems in a few years. Today, Triple-DES is exportable under the regulations described above.

Q22. I want to use DNAT with multiple original IPs, but my external NIC has just one IP. How can I do this?

A22. Make sure that the request reaches the RouteFinder, and then use DNAT to redirect the request to the Web servers. There are two ways to do this:

1. Bind an alias to the external interface, so that it answers ARP requests for this address and the packets are sent to the MAC address of this NIC. You can do this in **Network Setup > Interface** (refer to Chapter 3 of this manual).
2. Tell your router to send those packets directly to the RouteFinder's interface by adding a static routing entry to the RouteFinder.

Q23. My FTP clients want to use FXP transfers on my Server. How can I do that?

A23. For a fully functional FTP server (able to do FXP), the RouteFinder's "stateful inspection" function is not enough. Due to security concerns, the RouteFinder will only allow data connections from and to the same client IP as the control connection.

The example below shows how to make a "glftpd" server work behind a RouteFinder, which does both packet filtering and DNAT. The general principle applies to all other FTP servers too, so you can use it even if you use another server daemon.

Let's assume that you have **glftpd** set up in your LAN on address 192.168.1.10 with control port 23456. Your external, official IP on the RouteFinder is 1.2.3.4.

Go to **Networks & Services > Networks** and define the host entries for FTP server and external RouteFinder interface:

FTP_Server 192.168.1.10 255.255.255.255
ASL_Extern 1.2.3.4 255.255.255.255

Go to **Networks & Services > Services** and define entries for the control connection and the passive mode port range that the RouteFinder will use.

FTP_ALTControl TCP 1024:65535 23456
PASV_Range TCP 1024:65535 3000:4000

Note that we selected the ports from 3000-4000 to be our passive connection range in this example. You should select a range matching your setup, do not make it too small, and make sure you do not need any ports in this range for other services.

Go to **Packet Filters > Packet Filter Rules** and add the following rules:

Any FTP_ALTControl FTP_Server Allow

This rule allows connections of clients to the FTP server.

FTP_Server Any Any Allow

This rule allows the FTP server to make outgoing connections to clients, thus enabling the PORT command.

Any PASV_Range FTP_Server Allow

This rule allows connections from clients to the passive port range of the FTP server (needed to make passive mode work).

Add the DNAT rules. Go to **Network Setup > DNAT** and add the following definitions:

ASL_extern FTP_ALTControl FTP_Server FTP_ALTControl

ASL_extern PASV_Range FTP_Server PASV_Range

The RouteFinder setup is done. However, the FTP server does not know that it is placed behind a DNAT firewall, and thus will give out his 192.168.1.10 address when replying to a PASV command. In addition, we must tell it only to use the ports in our PASV_Range for passive connections.

Nearly all FTP servers have configuration options to set the IP and port range used for passive mode. In this case with **glftpd**, these are the options:

pasv_addr 1.2.3.4 1

pasv_ports 3000 4000

See ***glftpd.docs*** for more info on those configuration options, or check the docs of your particular FTP server if you use another daemon.

Q24. Do I need to add routes for my connected networks?

A24. No, you never have to add routes for networks in which your RouteFinder is a member. These so-called "Interface Routes" are automatically added by the RouteFinder itself.

Q25. I have DNAT set up but I cannot connect to the translated services. What's up?

A25. You may need to set packet filter rules to allow the traffic. When using DNAT, you must allow the traffic according to the characteristics BEFORE the translation.

For example:

If you translate **1.2.3.4:80** into **192.168.1.10:80**, you must allow **Any->1.2.3.4 port 80 TCP** (http).

When using SNAT, you must allow the traffic according to the characteristics after the translation. For example:

If you translate **SRC 192.168.10.1** into **SRC 1.2.10.1**, you must allow **1.2.10.1 -> any -> any**.

(Note that these are examples only!)

Q26. What does SOCKS stand for?

A26. SOCK-et-S was an internal development name that remained after release.

Q27. How is SOCKS V5 different from SOCKS V4?

A27. SOCKS V4 does not support authentication and UDP proxy. SOCKS V5 supports a variety of authentication methods and UDP proxy.

Q28. Does SOCKS V5 work with SOCKS V4?

A28. The SOCKS V5 protocol does not support SOCKS V4 protocol.

Q29. Where can I get SOCKS?

A29. SOCKS V4 implementation is available through anonymous ftp from ftp://ftp.nec.com:/pub/socks/. NEC's SOCKS V5 Both packages include clients for *telnet, ftp, finger,* and *whois*.

Other clients are available at ftp://ftp.nec.com:/pub/socks/

Q30. Are there any SOCKS-related mailing lists?

A30. Yes, there are SOCKS-related mailing lists for socks, socks5, and sockscap. To join the SOCKS mailing list, send an email message to: majordomo@socks.nec.com with no subject line and a one line body: subscribe <mailing-list> <your@email.address>

Correspond with members of the list by sending email to: <mailing-list>@socks.nec.com .

All three mailing lists are archived at /mail/socks/, /mail/socks5/, and /mail/sockscap/ .

Q31. Does SOCKS handle UDP?

A31. SOCKS V5 does, SOCKS V4 does not. NEC's SOCKS V5 Reference Implementation includes a socksified archie client program that is a UDP application.

Q32. How does SOCKS interact with DNS?

A32. For SOCKS version 4.2 and earlier, SOCKS V4 clients MUST resolve local and Internet host IP addresses. Configure DNS so that the SOCKS clients' resolver can resolve the addresses. Multiple DNS servers require special arrangements.

For the extended SOCKS version 4.3, SOCKS V4 clients can pass the unresolved addresses to the SOCKS V4 extended servers for resolution.

For SOCKS V5, the clients can pass unresolved host names to SOCKS V5 servers to resolve. SOCKS will work if the SOCKS V5 client or SOCKS V5 servers can resolve a host.

Q33. What is a single-homed and multi-homed firewall?

A33. A multi-homed firewall has multiple network interfaces and does not forward packets. Single-homed firewalls have one network interface card. You would use a single-homed firewall with a choke router that filters packets not originating from the SOCKS server.

Q34. Is there an RFC for SOCKS?

A34. There is no official RFC for Version 4 of the protocol. There are two documents describing Version 4: SOCKS V4 protocol and extension to SOCKS V4 protocol. There are three RFCs for SOCKS V5 related protocols:
RFC1928 - Describes SOCKS Version 5 protocol, also known as Authenticated Firewall Traversal (AFT).
RFC1929 - Describes Username/Password authentication for SOCKS V5.
RFC1961 - Describes GSS-API authentication for SOCKS V5

Q35. Why does the password echo when I run RFTP?

A35. The password only echoes for anonymous ftp. This is considered a feature.

Q36. What causes the log message *incompatible version number: 71*?

A36. Socks displays this log message when someone tries to use the SOCKS server as an HTTP proxy. ASCII code 71 is the letter "G", the first letter of an HTTP/1.0 request.

Chapter 9 – Troubleshooting

1. Review the RouteFinder FAQs in the previous section.

2. Verify that the pre-installation requirements are met. Refer to Chapter 2 of this manual.

3. Verify that the Administrations PC requirements are met (correct Default Gateway configuration, using an HTTPS-compatible Browser, JavaScript and Cascading Style active, and Proxies deactivated in the browser).

4. If you can't establish a connection and the message "***Error: The <software> is not reachable from the local network***" is displayed, try the following:
   - verify IP Addresses in the software are correctly configured (Chapter 3)
   - verify IP Address of the Client PC is correctly configured (Appendix F or G)
   - verify Default Gateway of the Client PC is correctly configured (Chapter 3)
   - verify proper Network Cable installation (Chapter 2)

5. Check for updates to the product documentation on the Multi-Tech web site at http://www.multitech.com/DOCUMENTS/.

6. To troubleshoot TCP/IP connections in Windows 2000, use the **Ping**, **Tracert**, and **Pathping** commands. The Ping command sends an Internet Control Message Protocol (ICMP) packet to a host and waits for a return packet, listing the transit time. If there isn't a return packet, Ping indicates that with a Request Time Out message. The Tracert command traces the route between two hosts and can be useful in determining where in the route a communications problem is occurring. Windows 2000 provides the **Pathping** command, which combines the features of Ping and Tracert and adds additional features to help you troubleshoot TCP/IP connectivity problems. **Pathping** sends packets to each router between two hosts and displays a report based on the return packets it receives. This report helps determine which routers in the path are experiencing problems. Check the Lost/Sent columns for an indication of the router experiencing problems. A particular router sustaining a high loss percentage rate is a reasonable indicator that there's a problem with that specific router. Type **PATHPING /?** at the command prompt to view the syntax for Pathping. **NOTE**: There is no **-r** switch; however, there is an **-R** switch (uppercase) that tests to determine if each hop is RSVP-aware. Also, the **-t** switch should be **-T** (uppercase).

7. If you use Internet Connection Sharing (ICS) or demand-dial router connections, and you have the problem of your client computer timing out while waiting for the ICS/demand-dial router to establish the connection. For example, your Web browser might report your home site as unreachable because TCP times out before the server can establish the connection. TCP sets a retransmission timer when it attempts the first data transmission for a connection, with an initial retransmission timeout value of 3 seconds. TCP doubles the retransmission timeout value for each subsequent connection attempt, and by default attempts retransmission twice. By default, the first attempt is made at 3 seconds, the second at 3+6 seconds, and the third at 3+6+12 seconds, for a maximum timeout of 21 seconds. Increasing the initial retransmission timer to 5 seconds would result in a total maximum timeout of 5+10+20, or 35 seconds.
   For Windows 2000 and Windows NT 4.0 clients, the initial TCP retransmission timeout is defined by the registry value HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\InitialRtt.
   The InitialRtt value is a REG_DWORD with a valid range from 0-65535 and specifies the timeout in milliseconds. The number of connection attempts is defined by the registry setting HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\TcpMaxDataRetransmissions.
   The TcpMaxDataRetransmissions value is also a REG_DWORD with a valid range of 0-65535.
   Caution: Make sure you have verified backup before you change these registry values.

8. If you are using an external keyboard connected to the RouteFinder's PC board using the **KB1** 6-pin female MiniDIN connector, make sure that you are not using an adapter cable (e.g., a 6-pin DIN to 6-pin miniDIN adapter cable).

9. Observe the RouteFinder front panel LEDs. Verify that the **LAN**, **WAN**, and/or **DMZ** LEDs indicate proper RouteFinder operation in terms of the Ethernet **LINK** integrity, transmit/receive activity (**ACT** LED), and speed (**100 MB** /10 MB). Refer to the front panel LEDs description in Chapter 1 of this manual.

10. For problems with RouteFinder filter rules, run **Statistics & Logs > Packet Filter > Filter Livelog** to view the RouteFinder's defined filter rules, system-generated filter rules, and filter violations.
    The Filter LiveLog supervises the packet filter and NAT rules. The Packet Filter log shows the packets that have not successfully passed the rule set of the packet filter.
    Click **Open Packet Filter LiveLog**; a window opens with the rule violations listed in order of occurrence.
    Note: Packets dropped by the **Drop** setting in **Packet Filters > Packet Filter Rules** do not appear in the **Packet Filter Livelog**.

11. Attach a monitor and keyboard to the RouteFinder for monitoring and debugging (refer to Chapter 5 of this manual for keyboard and monitor connection information).

12. Run the applicable **Statistics & Logs** function for the RouteFinder's status and performance:
    Uptime: length of continuous RouteFinder operation and date last booted
    Hardware: CPU, RAM, and Swap utilization
    Network: the internal network, NICs, Routing Table, and active Internet connections traffic
    Interfaces: displays network traffic on each interface - LAN, WAN, DMZ
    SMTP Proxy: displays email usage and status
    Accounting: calculates and displays external NIC IP packet byte counts
    Self Monitor: provides email notification of system-level issues
    IPSec: displays VPN information
    PPTP: displays processes and error messages
    Packet Filters: displays defined filter rules, system-generated rules, and filter violations
    Port Scans: disables and logs attempted port scans
    View Logs: displays a list of log files maintained by the RouteFinder
    HTTP Access: displays a list of users and the Internet sites visited by them
    Refer to Chapter 3 of this manual for **Statistics & Logs** menu information.

Appendix A – Disposition of Events for the RouteFinder v3.2x

For ICSA Certification
Based on
The Modular Firewall Certification Criteria
Baseline module - version 4.0

Revision History

Date	Revision	Remarks/Changes
16-Aug-2004	R1	Baseline document

Table of Contents

Table of Figures

1. Abstract

Disposition of Events

The LVPN RouteFinder 3.2x provides logging capabilities for various types of Access requests to the product.

The logging is classified as follows:

- Inbound Access Requests (LO1.A)
- Outbound Access Requests (LO1.B)
- Access Requests to Firewall Violating Security Policy (LO1.C)
- Access Requests Through Firewall Violating Security Policy (LO1.D)
- Administrative Authentication Log (LO1.E)
- Admin Port Access Requests (LO1.F)
- Startup History (LO1.G)
- User Defined Logs.
- Fragmented Packets Log. (ST6)

Access Request

An **Access Request** is the first packet arriving at the interface to which the security policy is applied. All subsequent packets that are part of an ongoing session are not termed as access requests since an Access Request is the first packet that establishes a session. Logging of an Access Request implies logging of the first packet of a session. Subsequent packets are not logged.

Inbound Access Request

Each access request from the external network to the box for any services hosted by the box or hosted by an internal server and have to pass through the firewall is termed as an inbound access request. Requests received on the WAN interface are termed **inbound access request**. If the WAN interface is down and the dial backup PPP link is up, then a request received on the PPP interface to the firewall will be termed **inbound request access**.

Access requests logged as Inbound Access Request correspond to LO1.A of Baseline module - version 4.0, ICSA Labs.

Figure 1 shows Inbound Access diagram
Figure 2 shows a snapshot of Inbound Access.
Figure 3 shows a snapshot of Inbound Access with DNAT and Connection Tracking.

Outbound Access Request

Each access request from the internal network (LAN/DMZ) to the external network (WAN) that passes through the firewall is termed as an Outbound Access Request. All requests routed out through the WAN interface to servers connected on or through the WAN Interface are considered **Outbound Access Requests**.

Access requests logged as Outbound Access Request correspond to LO1.B of Baseline module - version 4.0, ICSA Labs.

Figure 4 shows Outbound Access diagram.
Figure 5 shows a snapshot of Outbound Access
Figure 6 shows a snapshot of Outbound Access with connection tracking.

Access Requests through Firewall Violating Security Policy

An access request that traverses (routed through the firewall) but has to be dropped due to security restriction is logged as **Through Firewall dropped**.

Access requests logged as Access Request through Firewall Violating Security Policy correspond to LO1.C of Baseline module - version 4.0, ICSA Labs

Figure 7 show a snapshot of Through Firewall Dropped.

Access Request to Firewall Violating Security Policy

An Access request to the firewall can be dropped due to security restrictions. Each of these access requests is logged as **To Firewall Dropped**.

Access requests logged as Access Request to Firewall Violating Security Policy correspond to LO1.D of Baseline module - version 4.0, ICSA Labs.

Figure 8 shows To Firewall dropped diagram.
Figure 9 shows a snapshot of To Firewall Dropped.

Administrative Authentication Log

All successful and failed attempts to login to the VPN can be logged. The attempts are logged as Administrative Authentication Log.

Administrative Authentication Log corresponds to LO1.E of Baseline module - version 4.0, ICSA Labs.

Figure 10 shows a snapshot of Administrative Authentication Log.

Admin Port Access Requests

All requests to the Administrative port (HTTPS/HTTP to the box using the WEB GUI) are logged as Admin Port Traffic. Access requests logged as Admin Port Access requests correspond to LO1.F of Baseline module - version 4.0, ICSA Labs.
Figure 11 shows a snapshot of Admin Port Access log.

Startup History

The system startup Timestamp is logged as **Startup History**. Startup History corresponds to LO1.G of Baseline module - version 4.0, ICSA Labs.
Figure 12 shows a snapshot of Startup History.

User Defined Log

User defined logging is classified as *User* logs. Administrators can log packets using the **Packet Filers > Add User Defined Packet Filter Rules** and selecting **LOG** as the action.
Note: User logging is allowed only on routed packets.
Figure 13 shows a snapshot of user defined log.

Fragmented Packets Log

Fragments packets can be logged as **Dropped Fragmented**. Logging of **Dropped Fragmented Packets** can be configured through **Packet Filters > Advanced > Drop Fragmented Packets**. Logging is allowed only if fragments are dropped.
Figure 14 shows a snapshot of Fragmented Packets log.

ICMP information

Information about ICMP requests is available in the remarks. *Type* and *Code* information is displayed after the event type. ICMP information meets requirement LO2.G of Baseline module - version 4.0, ICSA Labs.
Figure 15 shows a snapshot with ICMP information.

II. Inbound Access Log

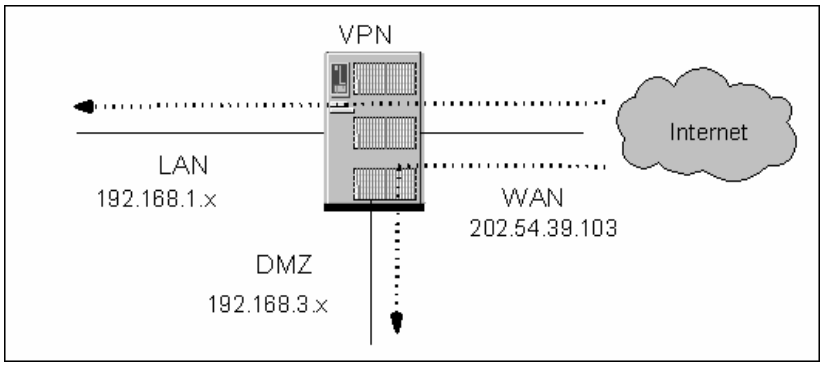


Figure 1 – Inbound Access

Log Display - Microsoft Internet Explorer

Sl No	Date	Time	Source IP	Destination IP	Protocol	Source port	Destination port	
1	11 Aug 2004	18:21:13	204.26.122.9	202.54.39.103	TCP	31108	53	Inbound Accepted
2	11 Aug 2004	18:31:13	204.26.122.9	202.54.39.103	TCP	41216	53	Inbound Accepted

Figure 2 – Snapshot of Inbound Access Log

Description of Figure 2

The Access request originated from the source (204.26.122.9) to the destination (204.54.39.103) is accepted by the candidate firewall. Classified as **Inbound Accepted**.

Inbound Access (DNAT with Connection Tracking)

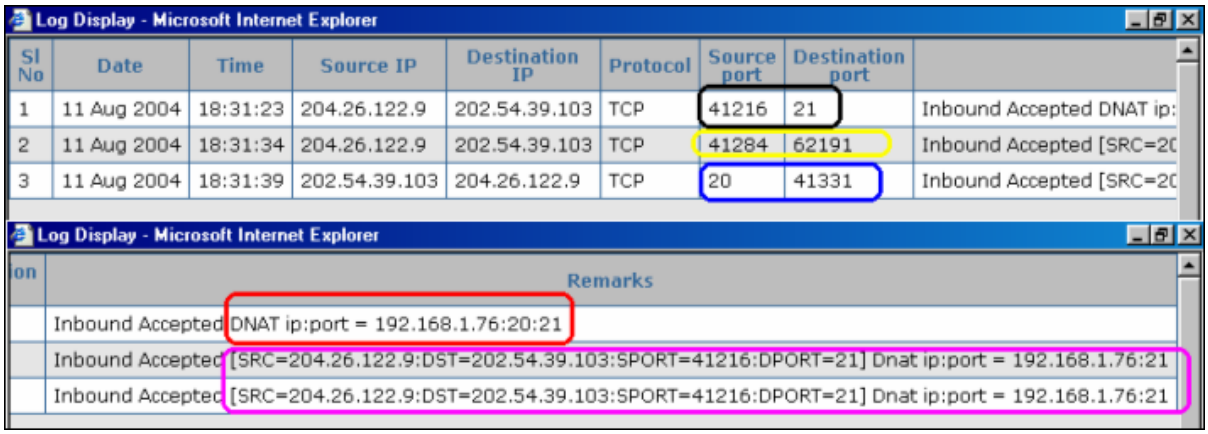


Figure 3 – Inbound Access (DNAT with Connection Tracking)

Description of Figure 3

The Access request originated from the source (204.26.122.9) to the destination (204.54.39.103), which is further DNATTED to the ip-address 192.168.1.76 on port 20:21.

The above figure illustrates a capture of the FTP service.

- Slno 1, in the above snapshot corresponds to the control connection (Remarks in the second half of the snapshot is a continuation of the capture).
  Remarks:
  "**Inbound Accepted DNAT ip:port = 192.168.1.76:20:21**"
  Src: 204.26.122.9, **Dst:** 202.54.39.103, **DNATTED to** 192.168.1.76 on Port 20:21.
- Slno 2, corresponds to a PASV Data connection. (Src:204.26.122.9, destined to 202.54.39.103, which in turn is DNATTED to 192.168.1.76 on port 62191).
  Remarks:
  "**Inbound Accepted**
  [SRC=204.26.122.9:DST=202.54.39.103:SPORT=41216:DPORT=21]
  Dnat ip:port = 192.168.1.76:21"
  - **Inbound Accepted –** Inbound Log
  - [SRC=204.26.122.9:DST=202.54.39.103:SPORT=41216:DPORT=21] – This corresponds to the "**CONTROL connection information**" for this data connection.
  - Dnat ip:port = 192.168.1.76:21" – This corresponds to the "**CONTROL connection's DNATTED ipaddress**" for this data connection.
- Slno 3, corresponds to the ACTIVE Data connection originated from 192.168.1.76 (on SRC-PORT 20), which is masqueraded to a SRC:202.54.39.103 at the WAN interface of the candidate firewall, destined to 204.26.122.9.
  Remarks:
  "**Inbound Accepted**
  [SRC=204.26.122.9:DST=202.54.39.103:SPORT=41216:DPORT=21]
  Dnat ip:port = 192.168.1.76:21"
  - **Inbound Accepted –** Inbound Log
  - [SRC=204.26.122.9:DST=202.54.39.103:SPORT=41216:DPORT=21] – This corresponds to the "**CONTROL connection information**" for this data connection.
  - Dnat ip:port = 192.168.1.76:21" – This corresponds to the "**CONTROL connection's DNATTED ipaddress**" for this data connection.

III. Outbound Access Log

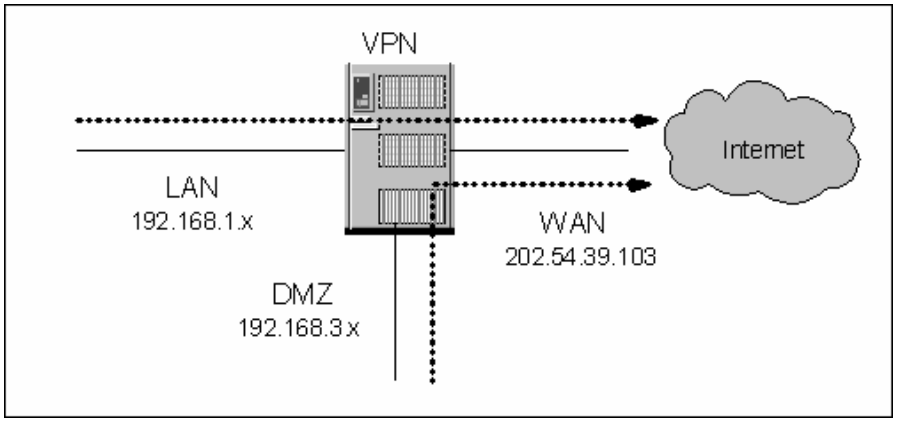


Figure 4 – Outbound Access

Log Display - Microsoft Internet Explorer

Sl No	Date	Time	Source IP	Destination IP	Protocol	Source port	Destination port	
1	11 Aug 2004	18:31:43	192.168.1.76	204.26.122.9	TCP	47945	22	Outbound
2	11 Aug 2004	19:04:08	192.168.1.212	195.220.108.108	TCP	32823	21	Outbound

Figure 5 – Snapshot of Outbound Access Log

Log Display - Microsoft Internet Explorer

Sl No	Date	Time	Source IP	Destination IP	Protocol	Source port	Destination port	
1	11 Aug 2004	18:31:43	192.168.1.76	204.26.122.9	TCP	47945	22	Outbound
2	11 Aug 2004	19:04:08	192.168.1.212	195.220.108.108	TCP	32823	21	Outbound
3	11 Aug 2004	19:04:29	195.220.108.108	192.168.1.212	TCP	20	32824	Outbound [SRC=192.1
4	11 Aug 2004	19:04:32	192.168.1.212	195.220.108.108	TCP	32825	41545	Outbound [SRC=192.1
5	11 Aug 2004	19:11:10	192.168.1.76	205.156.51.200	TCP	48020	80	Outbound
6	11 Aug 2004	19:11:11	192.168.1.76	209.132.177.110	TCP	48021	443	Outbound
7	11 Aug 2004	19:21:10	192.168.1.76	205.156.51.200	TCP	48030	80	Outbound

Log Display - Microsoft Internet Explorer

Active Connection

Passive Connection

n IP	Protocol	Source port	Destination port	Remarks
.9	TCP	47945	22	Outbound
8.108	TCP	32823	21	Outbound
212	TCP	20	32824	Outbound [SRC=192.168.1.212:DST=195.220.108.108:SPORT=32823:DPORT=21]
8.108	TCP	32825	41545	Outbound [SRC=192.168.1.212:DST=195.220.108.108:SPORT=32823:DPORT=21]
.200	TCP	48020	80	Outbound
7.110	TCP	48021	443	Outbound
.200	TCP	48030	80	Outbound

Figure 6 – Snapshot of Outbound Access Log (with Connection Tracking)

Description of Figure 6

The FTP Access request originated from the source (192.168.1.212 [SlNO 2]) to the destination (195.220.108.108). The above figure illustrates a capture of FTP service.

- Slno 2, in the above snapshot, corresponds to the control connection (Remarks in the second half of the snapshot is a continuation of the capture).
  Remarks:
  "**Outbound**"
  Src: 192.168.1.212, **Dst:** 195.220.108.108 on **Port:** 21.
- Slno 3 corresponds to a ACTIVE Data connection, originated by the FTP Server: 195.220.108.108, destined to: 192.168.1.212, on destination port: 32824
  Remarks:
  "**Outbound**
  [SRC=192.168.1.212:DST=195.220.108.108:SPORT=32823:DPORT=21]"
  - **Outbound –** Outbound Log
  - [SRC=192.168.1.212: DST=195.220.108.108: SPORT=32823: DPORT=21]" – This corresponds to the **CONTROL connection information** for this data connection.
- Slno 4 corresponds to the PASV Data connection originated from 192.168.1.212 destined to 195.220.108.108.
  Remarks:
  "**Outbound**
  [SRC=192.168.1.212:DST=195.220.108.108:SPORT=32823:DPORT=21]"
  - **Outbound –** Outbound Log
  - [SRC=192.168.1.212: DST=195.220.108.108: SPORT=32823: DPORT=21]" – This corresponds to the **CONTROL connection information** for this data connection.

IV. Access Requests through Firewall Dropped

Log Display - Microsoft Internet Explorer

Sl No	Date	Time	Source IP	Destination IP	Protocol	Source port	Destination port	Remarks
1	12 Aug 2004	14:44:12	192.168.1.212	216.239.37.99	TCP	33123	8000	Traverse Firewall Dropped
2	12 Aug 2004	14:44:15	192.168.1.212	216.239.37.99	TCP	33123	8000	Traverse Firewall Dropped
3	12 Aug 2004	14:44:21	192.168.1.212	216.239.37.99	TCP	33123	8000	Traverse Firewall Dropped
4	12 Aug 2004	14:44:33	192.168.1.212	216.239.37.99	TCP	33123	8000	Traverse Firewall Dropped
5	12 Aug 2004	14:44:57	192.168.1.212	216.239.37.99	TCP	33123	8000	Traverse Firewall Dropped

Figure 7 – Snapshot of Through Firewall Dropped Log

V. Access Requests to Firewall Dropped

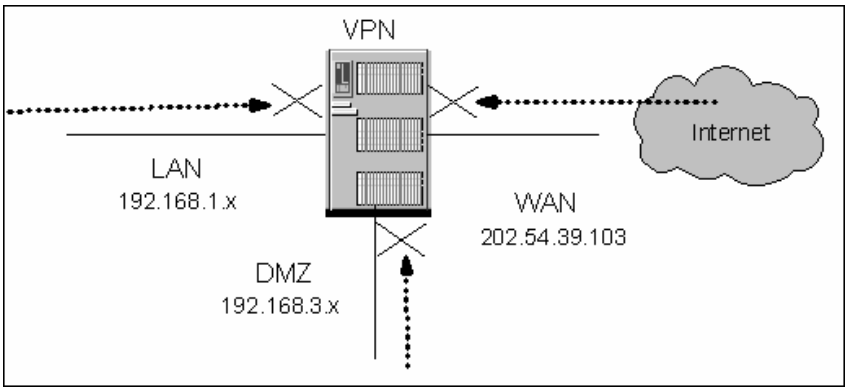


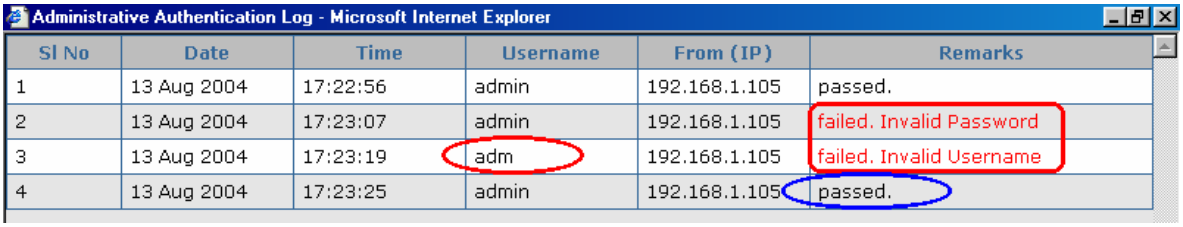
Figure 8 – Access Requests to Firewall Dropped

Log Display - Microsoft Internet Explorer

Sl No	Date	Time	Source IP	Destination IP	Protocol	Source port	Destination port	Remarks
1	11 Aug 2004	19:04:32	205.156.1.110	202.54.39.103	TCP	32825	80	To Firewall Dropped

Figure 9 – Snapshot of To Firewall Dropped Log

VI. Administrative Authentication Logs

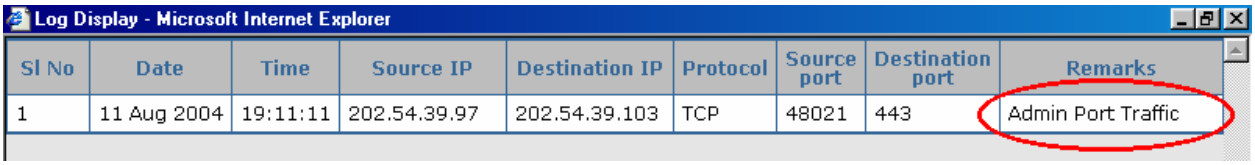


Administrative Authentication Log - Microsoft Internet Explorer

Sl No	Date	Time	Username	From (IP)	Remarks
1	13 Aug 2004	17:22:56	admin	192.168.1.105	passed.
2	13 Aug 2004	17:23:07	admin	192.168.1.105	failed. Invalid Password
3	13 Aug 2004	17:23:19	adm	192.168.1.105	failed. Invalid Username
4	13 Aug 2004	17:23:25	admin	192.168.1.105	passed.

Figure 10 – Snapshot of Administrative Authentication Log

VII. Admin Port Access Log



Log Display - Microsoft Internet Explorer

Sl No	Date	Time	Source IP	Destination IP	Protocol	Source port	Destination port	Remarks
1	11 Aug 2004	19:11:11	202.54.39.97	202.54.39.103	TCP	48021	443	Admin Port Traffic

Figure 11 – Snapshot of Admin Port Access Log

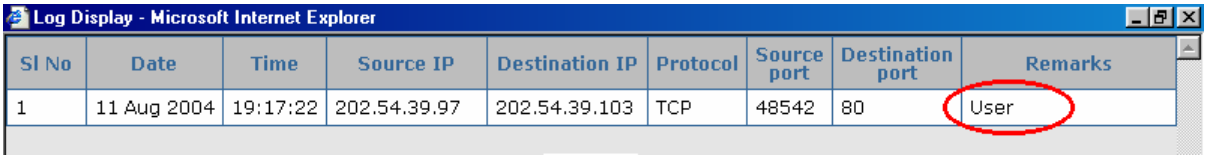
VIII. Startup History Log

Log Display - Microsoft Internet Explorer

System Startup History
Friday 13-August-2004 02:10:07 PM
Friday 13-August-2004 01:14:33 PM

Figure 12 – Snapshot of Startup History

IX. User Log

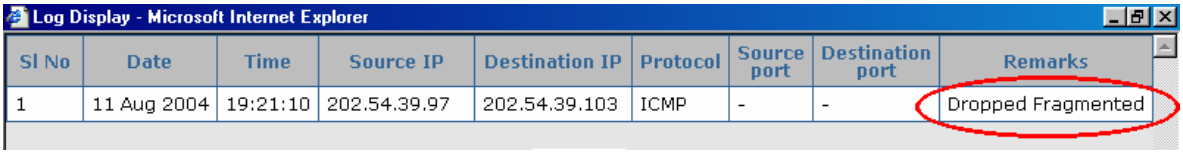


Log Display - Microsoft Internet Explorer

Sl No	Date	Time	Source IP	Destination IP	Protocol	Source port	Destination port	Remarks
1	11 Aug 2004	19:17:22	202.54.39.97	202.54.39.103	TCP	48542	80	User

Figure 13 – Snapshot of User Log

X. Fragmented Dropped Log

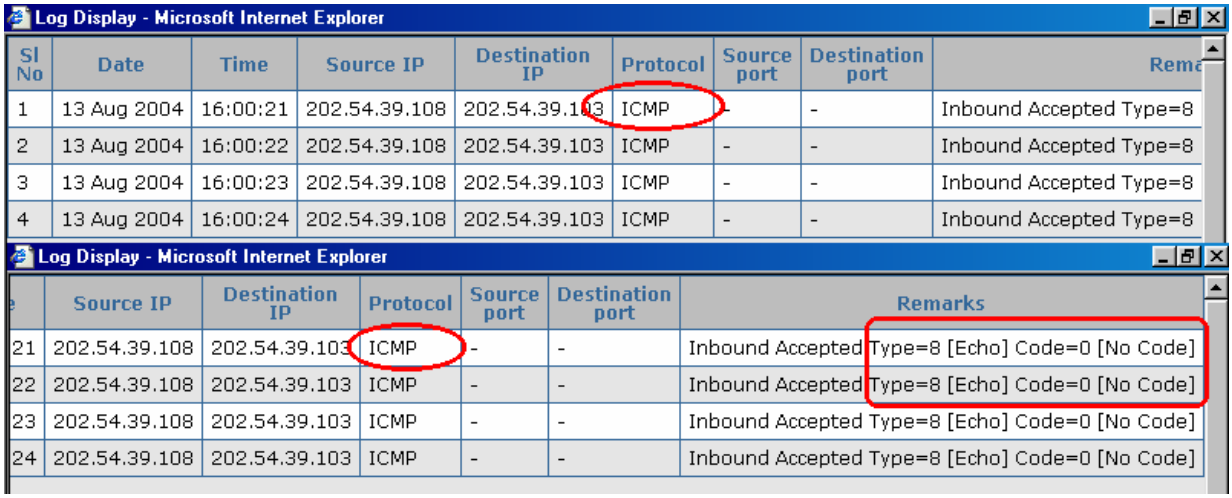


Log Display - Microsoft Internet Explorer

Sl No	Date	Time	Source IP	Destination IP	Protocol	Source port	Destination port	Remarks
1	11 Aug 2004	19:21:10	202.54.39.97	202.54.39.103	ICMP	-	-	Dropped Fragmented

Figure 14 – Snapshot of Fragmented Dropped Log

XI. ICMP Information



Log Display - Microsoft Internet Explorer

Sl No	Date	Time	Source IP	Destination IP	Protocol	Source port	Destination port	Rema
1	13 Aug 2004	16:00:21	202.54.39.108	202.54.39.103	ICMP	-	-	Inbound Accepted Type=8
2	13 Aug 2004	16:00:22	202.54.39.108	202.54.39.103	ICMP	-	-	Inbound Accepted Type=8
3	13 Aug 2004	16:00:23	202.54.39.108	202.54.39.103	ICMP	-	-	Inbound Accepted Type=8
4	13 Aug 2004	16:00:24	202.54.39.108	202.54.39.103	ICMP	-	-	Inbound Accepted Type=8

Log Display - Microsoft Internet Explorer

	Source IP	Destination IP	Protocol	Source port	Destination port	Remarks
21	202.54.39.108	202.54.39.103	ICMP	-	-	Inbound Accepted Type=8 [Echo] Code=0 [No Code]
22	202.54.39.108	202.54.39.103	ICMP	-	-	Inbound Accepted Type=8 [Echo] Code=0 [No Code]
23	202.54.39.108	202.54.39.103	ICMP	-	-	Inbound Accepted Type=8 [Echo] Code=0 [No Code]
24	202.54.39.108	202.54.39.103	ICMP	-	-	Inbound Accepted Type=8 [Echo] Code=0 [No Code]

Figure 15 – Snapshot of Log with ICMP Information

Appendix B – The RouteFinder Rescue Kernel

What Is a Rescue Kernel?

Rescue Kernel is a software program that allows you to reinstall the RouteFinder software without connecting the CD-ROM drive and using the RouteFinder software CD.

The Rescue Kernel can be installed on any of the RF6xx and RF7xx hardware, and it can be installed under version of the RouteFinder software. Once installed, and in case the hard drive will not boot or has been corrupted, Rescue Kernel will allow you to reinstall the ISO image also without connecting the CD-ROM drive and using the RouteFinder software CD.

With the Rescue Kernel you can configure the WAN IP and default gateway. You can perform everything remotely without having to be onsite. After the reinstallation is complete, you can use the RouteFinder software to access the WAN IP from the Internet assuming the public IP and default gateway were configured properly.

Before You Start

1. Check to See If Rescue Kernel Is Already Installed

Check to see if Rescue Kernel is already installed in your RouteFinder. To determine whether or not Rescue Kernel is already installed, use one of the following two methods:

- If you /boot directory has a file named creat_netinstall_cfg, then the Rescue Kernel is installed.

  OR

- Connect a keyboard and monitor to your RouteFinder. When you power on the RouteFinder, if you see that the LILO prompt pauses for a few seconds and, during the pause, if you can see the Boot: prompt when you press the ALT+TAB keys, then the Rescue Kernel is installed.

2. Configuration Backup

Backup your current RouteFinder configuration file and note the software version you are currently running.

3. Record License Key Numbers

- Locate you System license key and write it down. You will need this key after the software is installed.
- Locate your URL license key and write it down. You will need this if you planning to use the URL filter.
- If you have purchased and use the anti-virus options, locate your Anti-Virus license key file and write it down. You will need this to import the anti-virus software.

ISO Image Directions

The methods for reinstalling the RouteFinder software under Rescue Kernel will refer to the ISO image. You must follow these ISO image directions:

- When using RF600VPN hardware with a serial number **lower** than 9337635, DO NOT specify version 3.10 ISO image.
- When using RF600VPN hardware with a serial number **larger** than 9337635, DO NOT specify version 3.00 ISO image.
- When using RF760VPN hardware, DO NOT specify version 3.00 ISO image.
- LAN and WAN Interface configuration work during the Rescue Kernel setup only if you are reinstalling 3.1x ISO image and above.

Links You Will Need During the Install Process

Link to Download Windows FTP Server:
http://support.jgaa.com

Link to Download Windows WinSCP Client:
http://winscp.sourceforge.net/eng/

Link to Download Putty Telnet/SSH Client:
http://www.chiark.greeend.org.uk/

Three Methods for Performing the Software Reinstallation Using Rescue Kernel

Method 1 – This method uses no external server.

Method 2 – This method uses an external FTP server.

Method 3 – This method can be used if Method 1 and 2 fail.

Method 1 – How to Perform the Install Using No External Server

Assumptions: Your RouteFinder still has SSH access and you are still able to copy files onto the RouteFinder box.

1. Connect a workstation via the Ethernet to the LAN port of the RouteFinder box.
2. Use WinSCP to copy the RouteFinder ISO image to the RouteFinder **/home/loginuser** directory and then use the Putty utility to move it to the **/**root directory (see the ISO notes above).

   Please contact our support@multitech.com for a link to download the RouteFinder ISO image.

   Important Note: DO NOT perform Steps 3, 4 and 5 if Rescue Kernel is already installed. Check to see if the /boot directory contains the file named **create_netinstall_Cfg**. If this file is present, then Rescue Kernel is already installed.
3. Use SSH to access the RouteFinder box and use the WinSCP utility to copy **RFNetInstall.rpm** to the **/home/loginuser** directory. Download the **RFNetInstall.rpm** from **ftp://ftp.multitech.com/routers/RFNetInstall.rpm** (case sensitive).
4. Use the Putty utility to execute the following commands.
   Type in **rpm -ivh --nodeps /home/loginuser/RFNetInstall.rpm**.
5. Type in **rpm –e --justdb RFNetInstall** and **rm -f /home/loginuser/RFNetInstall.rpm**.
6. Type in **cd /boot** and **./create_netinstall_cfg**.

   At the following prompts, type the responses as indicated here:
   - Do you want to use the network install (y/n): n
   - Enter the ISO file name that is present in the root directory (/): RouteFinder3xx.iso.

     Make sure the file name is the same as Step 2 (case sensitive). See the ISO Notes at the beginning of this chapter.
   - Do you want an unattended install (y/n): y
   - Do you want to modify the current interface configuration (y/n): n

     If you answer y (yes), you can configure the LAN and WAN interface to match up with your network.

   Note: If any of these questions are answered incorrectly, execute the **./create_netinstall_cfg** command again and answer all questions correctly.
7. Type in **lilo -R RFNetInstall**.
8. Type in **reboot**.

9. Connect a monitor to the RouteFinder and monitor to make sure the install process does not show any problems. If there are problems during the install, you will need to use Method 3 to recover.

   If you do not have a monitor, you can listen for the following beep patterns:

   - The first three beeps. These beeps signal that the system is restarting in order to run Rescue Kernel.
   - The second five beeps. These beeps signal that the installation is done.
   - The third five beeps. These beeps signal that the software is running and is ready to use.

   Note: The install process will take sometime.

10. After installation is done and you have rebooted, you should be able to use WebAdmin to access the LAN port via IP address https://192.168.2.1

11. Configure your RouteFinder with live internet access. Then perform the live update to match the version you were running. Then import the backup configuration file.

Method 2 – How to Perform the Install Using an External FTP Server

Assumptions: Your workstation is on IP address 192.168.2.2.
The LAN port of RouteFinder is on ip address 192.168.2.1.

1. Connect a workstation via the Ethernet to the LAN port of the RouteFinder box.

2. Create an FTP server on the workstation and copy the RouteFinder ISO image file onto the FTP server root directory. Setup the FTP server with anonymous access. Test your FTP server with anonymous access so it shows the RouteFinder ISO image file in the root directory after an anonymous login. You can test your FTP server on the same machine by access IP ftp://127.0.0.1.

   Please contact our **support@multitech.com** for a link to download the RouteFinder ISO image.

   In the Jgaa FTP server, you will need to increase the number for allowing more FTP sessions and allowing more TCP connections. Change both of the settings to 10.

   Important Note: DO NOT perform Step 3, 4 and 5 if Rescue Kernel is already installed. Check to see if the /boot directory contains the file named **create_netinstall_Cfg**. If this file is present, then Rescue Kernel is already installed.

3. Use SSH to access the RouteFinder box and use WinSCP to copy **RFNetInstall.rpm** to **/home/loginuser** directory

4. Use the Putty utility to execute the following commands:
   Type in **rpm -ivh --nodeps /home/loginuser/RFNetInstall.rpm**.

5. Type in **rpm –e --justdb RFNetInstall** and **rm -f /home/loginuser/RFNetInstall.rpm**.

6. Type in **cd /boot** and **./create_netinstall_cfg**.

   At the following prompts, type the responses as indicated here:

   - Do you want to use the network install (y/n): y
   - Enter the interface to use (eth0/eth1/eth2) : eth0
   - Enter the IP address (IP/mask); e.g., (192.168.1.1/24): 192.168.2.1/24
   - Enter the default Gateway [Optional] :
   - Enter the Nameserver [Optional] :
   - Enter the protocol to be used (ftp/http/tftp) : ftp
   - For FTP, enter the URL (IP address or domain name): ftp://192.168.2.2
   - Enter the ISO path and filename: RouteFinder3xx.iso.
     Make sure the file name is the same as Step 2 (case sensitive). See the ISO notes at the beginning of this chapter.
   - Do you want an unattended install (y/n): y
   - Do you want to modify the current interface configuration (y/n): n
   - If you answer y (yes), you can configure the LAN and WAN interface to match up with your network.

   Note: If any of these questions are answered incorrectly, execute the **./create_netinstall_cfg** command again and answer all questions correctly.

7. Type in **lilo -R RFNetInstall**.
8. Type in **reboot**.
9. Connect a monitor to the RouteFinder and monitor to make sure the install process does not show any problems. If there are problems during the install, you will need to use Method 3 to recover.

   If you do not have a monitor, you can listen for the follow beep patterns:
   - The first three beeps. These beeps signal that the system is restarting in order to run the Rescue Kernel.
   - The second five beeps. These beeps signal that the installation is done.
   - The third five beeps. These beeps signal that the software is running and is ready to use.
10. The install process will take sometime depending on the method.
11. After installation is done and you have rebooted, you should be able to use WebAdmin to access the LAN port via IP address https://192.168.2.1
12. Configure your RouteFinder with live internet access. Then perform the live update to match the version you were running. Then import the backup configuration file.

Method 3 – How to Perform the Install If the Other Methods Fail or If the File Systems Are Corrupted

Use this method if Methods 1 and 2 have failed or if the file systems are totally corrupted and the RouteFinder can boot only with Rescue Kernel.

Assumption: Rescue Kernel is already installed in your system.

1. Set up an external FTP server. Refer to the steps above in Method 2.
2. Connect a monitor and keyboard to the RouteFinder box. During bootup, right after the BIOS messages, you must press <ALT+TAB> when you see the word **LILO**. You have only a few seconds, so you will have to be fast. Otherwise, the RouteFinder will boot into the regular software.
3. If <ALT+TAB> works, you will see a prompt. At the prompt, type in **RFNetInstall** (case sensitive). If **RFNetInstall** does not work, this means you do not have Rescue Kernel installed. In this case, you will need to reinstall the software using the CD method.
4. Rescue Kernel terminates after the install process. You can also terminate during the Rescue Kernel boot process by pressing Ctrl+C .
5. Then, at the prompt, type in the following:
   - **cd /boot**
   - **./create_netinstall_cfg** (See Step 6 in Method 2 for ./create_netinstall_cfg directions.)
     Note: If you need to set up FTP, see Step 2 in Method 2.
   - **reboot**
6. The install process will take sometime depending on the method you use.
7. After the installation is done and you have rebooted, you should be able to use WebAdmin to access the LAN port via IP address https://192.168.2.1.
8. Configure your RouteFinder with live internet access. Then perform the live update to match the version you were running. Then import the backup configuration file.

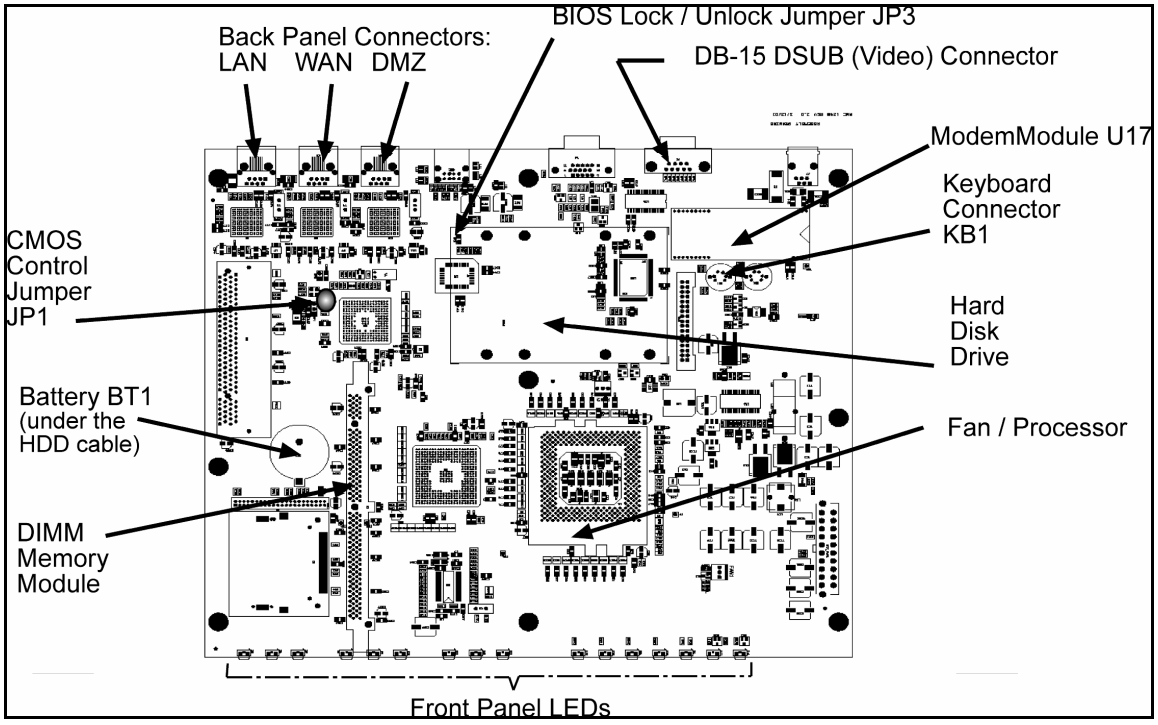
Appendix C – Board Components, Hardware Upgrades & Add-ons, Software Add-ons, Overnight Replacement

Board Components

The RouteFinder board components are illustrated and discussed below. **Note**: Several of the RouteFinder board components are user-configurable; however, please contact Tech Support before changing the component settings.

Notes:

- The board in the example shown below is for the RF660VPN.
- The hard drive mount for the RF760VPN is the same except that some of the board components differ.
- The hard drive mount for the RF600VPN is on the left side of the its board.



PC Board Component Descriptions

U17: Not used.

2.5"/20 GB/EIDE Hard Disk (HD) Drive: a mini hard disk drive that provides system storage. The HD drive can be upgraded in the field for additional storage, and can be replaced with a mini CD-ROM drive as well. The existing HD ribbon cable is terminated with a connector for the CD-ROM drive.
Note: Other hard disk drive capacities are available as options.

J6 Hard drive connector: J6 has an arrow to designate pin 1. The hard drive ribbon cable is terminated with a connector for the HD as well as a connector for substituting a CD-ROM drive.

850 Mhz INTEL® Celeron™ Processor: the microprocessor that provides processing power to the unit. The processor can be upgraded in the field for additional processing power. **On RF760VPN: 2GHZ Pentium 4**

256MB PC133 Non-ECC DIMM: the memory component for the unit. The DIMM memory module can be upgraded in the field for higher performance. Early RouteFinders had a 128MB PC100 Non-ECC DIMM.
On RF760VPN: 512MB DDR DIMM

VGA CRT connector: This connector allows attachment of a monitor for configuration and reporting purposes.

CN4 Floppy drive connector: The floppy drive connector (**CN4**) does not have a designator for pin 1.

Back Panel: the back panel contains the Fan, **POWER** plug, Power Switch (**| / o**), RJ-11 (**LINE**), DB-9 (**COM 1**), DB-15 High density DSUB (**VIDEO**), **USB** (Revision 1.1 compliant), RJ-45 (**DMZ**), RJ-45 (**WAN**), and RJ-45 (**LAN**) connections.

KB1 MiniDIN SVT1: KB1 is a 6-pin female PS/2 keyboard interface connector.

BT1 Battery: BT1 is a lithium battery that provides backup power for time keeping.
Caution: Danger of explosion if battery is incorrectly replaced. The lithium battery on the RouteFinder board provides backup power for the time-keeping capability. The battery has an estimated life expectancy of ten years. When the battery starts to weaken, the date and time may be incorrect. If the battery fails, the board must be sent back to Multi-Tech Systems for battery replacement.

JP1 CMOS control jumper: JP1 settings are Normal (default) or Clear CMOS.
For Normal short pins 1 and 2. For Clear CMOS short pins 2 and 3.

JP3: BIOS Lock / Unlock jumper: JP3 settings are IN: Unlocked and OUT: Locked (default).

Hardware Upgrades and Add-ons

This section provides the information needed to perform RouteFinder field upgrades.
Caution: Use industry-standard grounding supplies and procedures so that you do not damage the PC board or upgrade components.

Top Cover Removal

As the first step for all upgrade procedures, use this procedure to remove the RouteFinder top cover.

1. Turn off RouteFinder power and remove the RouteFinder power cord.
2. Remove all of the RouteFinder back panel cable connections.
3. Remove the retaining screws that secure the top cover to the chassis. Save the screws for top cover replacement.
4. Carefully slide the top cover forward and then off of the chassis, being careful not to catch the top cover on any cables or to bump any of the board components. You may want to use a small flat blade screwdriver to gently pry the top cover away from the chassis at the retaining screw hole near the middle of the back panel.
5. Perform the desired upgrade following the instructions in the following sections.
6. To replace the top cover, perform Steps 1-3 above in reverse order.

RF660VPN Processor Upgrade

The standard 566 Mhz INTEL® Celeron™ processor can be upgraded in the field up to a 850 MHz Celeron processor or up to an 850 MHz Pentium3™ processor.

1. Remove the RouteFinder top cover using the procedure earlier in this chapter.
2. Unplug the fan power plug from the FAN1 connector on the board.
3. Gently press down on the top of the metal fan retaining strip and unlatch it from the plastic retaining tab. Fan1 is mounted directly on top of the beige plastic Processor housing. Carefully remove Fan1 and the metal fan retaining strip and put them in a safe place for future replacement.
4. Unlatch the Processor housing by carefully moving the securing lever on the right side out away from the housing and lifting upward; this moves the securing lever from the LOCK to the FREE position, as printed on the beige plastic Processor housing.
5. Very carefully remove the existing processor from the processor socket.
6. Carefully insert the upgrade processor, following the processor manufacturer's instructions.
7. Perform steps 1 through 4 in reverse order.
8. Power up the RouteFinder and refer to Chapter 2 - Configuration.

Memory Upgrade

The standard 128-Mb memory module can be upgraded in the field to 256 MB.

1. Remove the RouteFinder top cover using the procedure earlier in this chapter.
2. Pull back on the beige plastic DIMM retaining tabs on both sides of the DIMM holder at M1.
3. Carefully remove the existing DIMM card.
4. Insert the upgrade DIMM card following the manufacturer's documentation.

Hard Disk Drive Upgrade

The standard 2.5" 20 GB EIDE Hard Disk Drive can be upgraded in the field to a higher capacity hard drive.

1. Remove the RouteFinder top cover using the procedure earlier in this chapter.
2. Disconnect the HD drive ribbon cable at the existing HD drive; note that the HD drive ribbon cable connects to all of the HD drive pins except the two sets of two pins on the far right.
3. Using a small Phillips screwdriver remove the four screws that fasten the HD drive to the HD drive-mounting bracket. Keep the four HD mounting screws.
4. Install the replacement HD drive into the HD drive-mounting bracket.
5. Fasten the HD drive using four HD mounting screws.
6. Re-connect the HD drive ribbon cable at the replacement HD drive; note that the HD drive ribbon cable connects to all of the HD drive pins except the two sets of two pins on the far right.

CD-ROM Drive Add-on

The Hard Disk drive ribbon cable is terminated with a connector for the HD drive, as well as a connector for connecting a CD-ROM drive. To connect a CD-ROM drive, perform the following procedure.

1. Remove the RouteFinder top cover using the procedure earlier in this chapter.
2. Remove the TY-RAP holding down the cable.
3. Remove the 44-pin - 40-pin converter from the cable.
4. Connect the CD-ROM drive to the CD-ROM connector at the end of the Hard Disk drive ribbon cable.

Keyboard Connection

KB1 is a keyed 6-pin MiniDIN PS/2 interface on the RouteFinder board used for connecting a keyboard. Perform the following steps to attach a keyboard to the unit for configuration and reporting.

1. Remove the RouteFinder top cover using the procedure earlier in this chapter.
2. Connect the keyboard to the **KB1** keyed connector.

Monitor Connection

Perform the following steps to attach a VGA monitor to the RouteFinder for configuration and reporting.

1. Remove the RouteFinder top cover using the procedure earlier in this chapter.
2. Connect the monitor to the RouteFinder back panel DB15 High Density **DSUB** connector using a DB9-to-DB15 cable.

Rack Mounting

The RouteFinder is shipped with four rubber feet for desktop applications, two rack mounting brackets, and four mounting screws.

Note: Rack Mount screws are provided to attach the brackets to the RouteFinder. It is up to you to provide the bracket-to-rack rack mounting screws that match your rack's thread size.

Use the rack manufacturer's documentation and procedure to safely and securely install the RouteFinder in almost any 19" rack.

Software Add-ons

Listed below are the software add-ons available for the RouteFinder:

SSH Sentinel IPSec VPN Client Software

The SSH Sentinel IPSec VPN Client software is available in 1-, 5-, 10- and 50-user packages. The RouteFinder provides SSH Sentinel client software (30-day trial Internet Pilot version with Static IP support). It allows client computer connection to the RouteFinder using PSK (Pre Shared Keys) in a Host-to-Net connection. (See the separate SSH IPSec Sentinel Reference Guide for a description of the SSH IPSec VPN client setup process.) To upgrade to the full 1-, 5-, 10- or 50-user Sentinel SSH IPSec VPN client package, order the applicable model (RFIPSC-5, RFIPSC-10, or RFIPSC-50) from Multi-Tech for the number of users that you require.

Model	Description
RFIPSC-1	SSH IPSec VPN Client 1-User License
RFIPSC-5	SSH IPSec VPN Client 5-User License
RFIPSC-10	SSH IPSec VPN Client 10-User License
RFIPSC-50	SSH IPSec VPN Client 50-User License
RFAVUPG	1-Year Email Anti-Virus Protection Upgrade

Email Anti-Virus Code

The RouteFinder is shipped with Email Anti-Virus code within the core software. Order model # RFAVUPG to obtain the software key that enables this Email Anti-Virus Protection subscription for a one-year time period. The one-year 'subscription' must be renewed to continue the anti-virus support. You will receive renewal notices from Multi-Tech prior to the end of your subscription.

The latest virus pattern updates can then be downloaded from the Multi-Tech server. The RouteFinder's auto-update feature lets it connect to the server and automatically download and install these new virus pattern files at user-defined intervals. See Chapter 3 for more Update Services information. The optional email virus protection subscription utilizes a high-performance, ICSA-tested, anti-virus engine which checks both incoming and outgoing email for viruses in real-time (See the Tracking section).

The RouteFinder Email Anti-Virus software is an optional purchase.

For a free 30-day evaluation, go to:
http://www.multitech.com/register/eval/

To purchase the one year RouteFinder Email Anti-Virus software upgrade, go to:
http://www.multitech.com/PRODUCTS/RouteFinderVPN/

If you purchased the RouteFinder Email Anti-Virus software and need to activate the option, go to:
http://www.multitech.com/register/rfavupg/

Complete and submit the form and a new license key will be emailed or faxed to you within 24 hours or the next business day. Included with your new license will be instructions for installing the new key.

Note: Anti-Virus Copyright

The RouteFinder Email Anti-Virus software is provided by Kaspersky Anti-Virus engine copyrighted by Kaspersky Labs.

Overnight Replacement Service

Although our products are known for their reliability, performance, and flexibility, we understand that mission-critical information must be accessible when your customers need it, where they need it, with no time for product failure. That is why we have developed the Multi-Tech Overnight Replacement Service for our U.S. customers to provide fast replacement for equipment failures. So fast, that delivery is made overnight!

Benefits of the program include:

- Reduces downtime
- Maximizes equipment reliability and availability
- Streamlines problem resolution
- Includes all overnight shipping charges
- One-time fee
- Two-year coverage for specified failed equipment
- Replacement equipment will be functionally equal
- Contract is renewable every two years*

If you have any questions regarding the program, contact customer service at 1-888-288-5470. You may also visit our Web site at www.multitech.com or purchase online at buy.multitech.com.

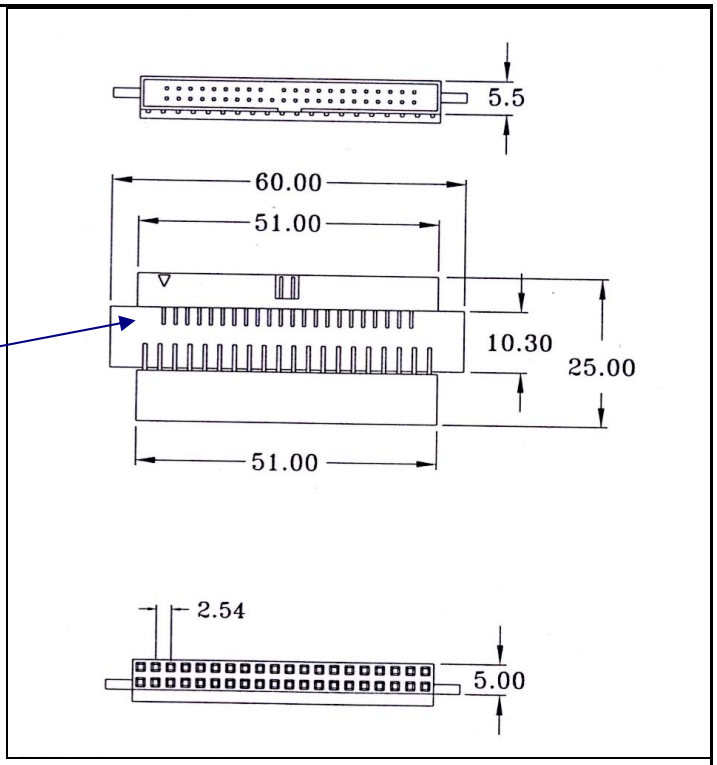
Appendix D – CD-ROM Drive Adapter and Pin Out

CD-ROM Drive Adapter Dimensions

Pin 1

Note: Pin 1 of the converter must match with the red line of the ribbon cable.

The adapter is polarity sensitive. It will not work if the adapter is inverted



CD-ROM Drive Adapter Pin Out

The 44 pin (m)-to-40 pin (f) adapter pin-out is shown below. **P1** is the 44-pin male header; **P2** is the 40-pin female box header.

P1	P2	P1	P2
1	1	21	21
2	2	22	22
3	3	23	23
4	4	24	24
5	5	25	25
6	6	26	26
7	7	27	27
8	8	28	28
9	9	29	29
10	10	30	30
11	11	31	31
12	12	32	32
13	13	33	33
14	14	34	34
15	15	35	35
16	16	36	36
17	17	37	37
18	18	38	38
19	19	39	39
		40	40

Appendix E – RouteFinder Maintenance

This section covers issues related to routinely maintaining the RouteFinder, including:

- Housekeeping
- Monitoring
- Updating

Housekeeping

Housekeeping includes the on-going list of tasks that you need to perform to keep your environment safe and clean. The three main housekeeping tasks that you'll need to revisit periodically are:

- **System backups** – This includes regular backups of RouteFinder configurations and reporting logs. Much of the system backup effort can be done automatically on the RouteFinder (refer to the System > Backup section in Chapter 3 of this manual).
- **Accounts management** – Includes adding new accounts correctly, deleting old ones promptly, and changing passwords regularly. You should arrange to get termination notification when someone leaves your organization (e.g., for your company's full-time and contract employees, or your university's graduating students). This should involve managing Certification and Key expiration dates, maintaining current email address or addresses for alerts and notifications (e.g., from the **Administration** menu), as well as maintaining the overall WebAdmin password from he **Administration** menu.
- **Shared Secret Maintenance** – Most secure protocols provide for mutual authentication (server-to-client and client-to-server). Most ways of doing this are based on the same process: each side "proves" that it can decrypt a value that only the "authentic" participant can know.
  This secret could be the private half of a public key / private key pair, or it could be a key used along with a symmetric algorithm. In both authentication methods each side sends the other an 'unpredictable' value, and then gets it back in a form that proves that the other side was able to decrypt it.

  Public key cryptography provides excellent data protection, but it's fairly slow. A convenient method is to use a temporary key (AKA, a session key) for most transactions, and then destroy the session key when the transaction is completed. Here, a secure protocol negotiates a session key that is used for a single transaction. The session key is still unpredictable and secure, but takes a lot less time to generate. However, when using the temporary (session) key method, it becomes important for the administrator to destroy quickly and systematically the shared secrets once they are used. Using *partial perfect forwarding secrecy* the shared secret is destroyed after a set period of time. When using perfect secret forwarding, the administrator is responsible for destroying used shared secrets.
- **Disk space management** – Includes timely 'cleanup' of random program and data files to avoid wondering if a program is a leftover from a previous user, or a required program needed for a new install, or a program that an intruder left behind as a 'present' for someone to open. Eliminating unneeded files will allow more room on the hard drive for important logs and reports.
- **Authentication Keys Maintenance** – Authentication keys need to be unpredictable, and random numbers can often be necessarily involved. You'll want to change authentication keys often, since the longer a key is used, the more likely it is to be discovered or accidentally disclosed.

Monitoring

Here you need to keep track of your system in terms of 'normal' usage so you can tell:

- If your RouteFinder is working.
- If your RouteFinder has been compromised.
- What kinds of attacks are being perpetrated.
- If your RouteFinder is providing the services your users need, or if upgrades or add-ons are needed.

To be proactive in solving these issues, keep track of usage reports and logs (refer to the sections on **User Authentication**, **Tracking**, and **Statistics & Logs** in Chapter 3). For information on RouteFinder upgrades and add-ons refer to the preceding section, **Software Upgrades and Add-ons**.

Updating

This involves keeping both yourself and your RouteFinder abreast of new bugs, new attacks and new patches, new tools and resources, etc. Much of the RouteFinder updating effort can be done automatically (refer to the **Tracking > Update Service** section in Chapter 3). Administrators can keep themselves current with mailing lists, news groups, security forums, etc. (Refer to the section on Pre-Installation Planning in Chapter 2 of this manual for additional sources of information).

The SANS Institute and the National Infrastructure Protection Center (NIPC) produced a document summarizing the Twenty Most Critical Internet Security Vulnerabilities. Thousands of organizations use the list to prioritize their efforts so they could close the most dangerous holes first. It is segmented into three categories: General Vulnerabilities, Windows Vulnerabilities, and Unix Vulnerabilities. The SANS/FBI Top Twenty list is valuable because the majority of successful attacks on computer systems via the Internet can be traced to exploitation of security flaws on this list. While manually checking a system for each of the listed vulnerabilities is possible, a more practical way to find UNIX and Windows vulnerabilities is to use an automated scanner.

Bob Todd, the author of the free Internet scanner SARA, created a version of SARA that finds and reports on the status of the SANS/FBI Top Twenty list. SARA's Top Twenty Vulnerability scanner is available from the Center for Internet Security (**www.cisecurity.org**). You can download a copy from this site.

Several commercial vulnerability scanners may also be used to scan for these vulnerabilities, and the SANS Institute maintains a list of all scanners that provide a focused Top Twenty scanning function at **www.sans.org**.

Appendix F – Ordering Accessories

SupplyNet, Inc. supplies replacement transformers, cables, and connectors for select Multi-Tech products. You can place an order with SupplyNet via mail, phone, fax, or the Internet at:

Mail: SupplyNet, Inc.
614 Corporate Way
Valley Cottage, NY 10989
Phone: 800 826-0279
Fax: 914 267-2420
Email: info@thesupplynet.com
Internet: http://www.thesupplynet.com

SupplyNet Online Ordering Instructions

1. Browse to http://www.thesupplynet.com. In the Browse by Manufacturer drop-down list, select Multi-Tech and click GO!
2. To order, type in the quantity, and click Add to Order.
3. Click Review Order to change your order.
4. After you have selected all of your items, click Checkout to finalize the order. The SupplyNet site uses Verisign's Secure Socket Layer (SSL) technology to ensure your complete shopping security.

Appendix G – Technical Support

Technical Support Contacts

Country	By Email	By Phone
France:	support@multitech.fr	(33) 1-64 61 09 81
India:	support@multitechindia.com	91 (124) 6340778
U.K.:	support@multitech.co.uk	(44) 118 959 7774
U.S. and Canada:	support@multitech.com	(800) 972-2439
Rest of the World:	support@multitech.com	(763) 717-5863

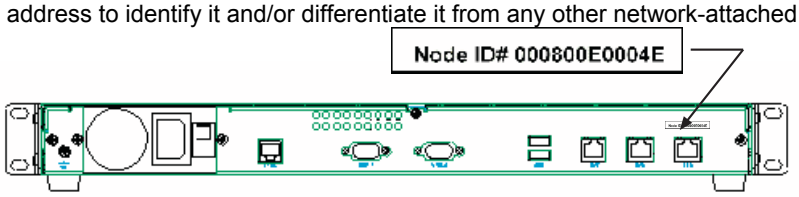
Internet Address: http://www.multitech.com
FTP Address: ftp://ftp.multitech.com.

Recording RouteFinder Information

Please fill in the following information on your Multi-Tech RouteFinder. This will help tech support in answering your questions. (The same information is requested on the Warranty Registration Card.)
Model No.: _____
Serial No.: _____
Software Version: _____
License Key No.: _____-_____-_____-_____
URL Filter Key _____

These numbers are located on the bottom of your RouteFinder. The Software Version is displayed at the top of the Home screen.

Provide the configuration information (e.g., Default Gateway and other IP addresses used) from the Address Table in Chapter 2 of this manual, as well as any available **LiveLog** or **Statistics & Logs** information.
Record the Node ID# from the RouteFinder's back panel; it may be required by the ISP for administration purposes or connection identification. Every device that contains an Ethernet NIC (Network Interface Card) has an assigned Media Access Control (MAC) address to identify it and/or differentiate it from any other network-attached device.



Also, note the status of your RouteFinder including LED indicators, screen messages, diagnostic test results, problems with a specific application, etc.

Appendix H – Multi-Tech Systems, Inc. Warranty and Repairs Policies

Multi-Tech Warranty Statement

Multi-Tech Systems, Inc., (hereafter "MTS") warrants that its products will be free from defects in material or workmanship for a period of two, five, or ten years (depending on model) from date of purchase, or if proof of purchase is not provided, two, five, or ten years (depending on model) from date of shipment.

MTS MAKES NO OTHER WARRANTY, EXPRESS OR IMPLIED, AND ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE HEREBY DISCLAIMED.

This warranty does not apply to any products which have been damaged by lightning storms, water, or power surges or which have been neglected, altered, abused, used for a purpose other than the one for which they were manufactured, repaired by Customer or any party without MTS's written authorization, or used in any manner inconsistent with MTS's instructions.

MTS's entire obligation under this warranty shall be limited (at MTS's option) to repair or replacement of any products which prove to be defective within the warranty period or, at MTS's option, issuance of a refund of the purchase price. Defective products must be returned by Customer to MTS's factory — transportation prepaid.

MTS WILL NOT BE LIABLE FOR CONSEQUENTIAL DAMAGES, AND UNDER NO CIRCUMSTANCES WILL ITS LIABILITY EXCEED THE PRICE FOR DEFECTIVE PRODUCTS.

Repair Procedures for U.S. and Canadian Customers

In the event that service is required, products may be shipped, freight prepaid, to our Mounds View, Minnesota factory:

Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, MN 55112 U.S.A
Attn: Repairs, Serial # _____

A Returned Materials Authorization (RMA) is not required. Return shipping charges (surface) will be paid by MTS to destinations in U.S. and Canada.

Please include, inside the shipping box, a description of the problem, a return shipping address (must have street address, not P.O. Box), your telephone number, and if the product is out of warranty, a check or purchase order for repair charges.

For out of warranty repair charges, go to COMPANY/Policies/warranty/

Extended two-year overnight replacement service agreements are available for selected products. Please call MTS customer service at (888) 288-5470 or visit our web site at COMPANY/Programs/overnight_replacement for details on rates and coverage's.

Please direct your questions regarding technical matters, product configuration, verification that the product is defective, etc., to our Technical Support department at (800) 972-2439 or email support@multitech.com. Please direct your questions regarding repair expediting, receiving, shipping, billing, etc., to our Repair Accounting department at (800) 328-9717 or (763) 717-5631, or email mtsrepair@multitech.com.

Repairs for damages caused by lightning storms, water, power surges, incorrect installation, physical abuse, or user-caused damages are billed on a time-plus-materials basis.

Repair Procedures for International Customers

(Outside U.S.A. and Canada)

Your original point of purchase Reseller may offer the quickest and most economical repair option for your Multi-Tech product. You may also contact any Multi-Tech sales office for information about the nearest distributor or other repair service for your Multi-Tech product. The Multi-Tech sales office directory is available at http://www.multitech.com/COMPANY/contact_us/

In the event that factory service is required, products may be shipped, freight prepaid to our Mounds View, Minnesota factory. Recommended international shipment methods are via Federal Express, UPS or DHL courier services, or by airmail parcel post; shipments made by any other method will be refused. Please include, inside the shipping box, a description of the problem, a return shipping address (must have street address, not P.O. Box), your telephone number, and if the product is out of warranty, a check in U.S. dollars drawn on a U.S. bank or your company's purchase order for repair charges. Repaired units shall be shipped freight collect, unless other arrangements are made in advance.

Please direct your questions regarding technical matters, product configuration, verification that the product is defective, etc., to our Technical Support department nearest you or email support@multitech.com. When calling the U.S., please direct your questions regarding repair expediting, receiving, shipping, billing, etc., to our Repair Accounting department at +(763) 717-5631 in the U.S.A., or email mtsrepair@multitech.com.

Repairs for damages caused by lightning storms, water, power surges, incorrect installation, physical abuse, or user-caused damages are billed on a time-plus-materials basis.

Repair Procedures for International Distributors

International distributors should contact their MTS International sales representative for information about the repair of the Multi-Tech products.

Please direct your questions regarding technical matters, product configuration, verification that the product is defective, etc., to our International Technical Support department at +(763)717-5863. When calling the U.S., please direct your questions regarding repair expediting, receiving, shipping, billing, etc., to our Repair Accounting department at +(763) 717-5631 in the U.S.A. or email mtsrepair@multitech.com.

Repairs for damages caused by lightning storms, water, power surges, incorrect installation, physical abuse, or user-caused damages are billed on a time-plus-materials basis.

Appendix I – Regulatory Compliance

EMC, Safety, and R&TTR Directive Compliance

The CE mark is affixed to this product to confirm compliance with the following European Community Directives:
Council Directive 89/336/EEC of 3 May 1989 on the approximation of the laws of Member States relating to electromagnetic compatibility.
and
Council Directive 73/23/EEC of 19 February 1973 on the harmonization of the laws of Member States relating to electrical equipment designed for use within certain voltage limits;
and
Council Directive 1999/5/EC of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity.

FCC Part 15 Regulation for the Modem Operation

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.
This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference that may cause undesired operation.

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

FCC Part 68 Telecom for the Modem Operation

1. This equipment complies with Part 68 of the Federal Communications Commission (FCC) rules. On the outside surface of this equipment is a label that contains, among other information, the FCC registration number. This information must be provided to the telephone company.
2. As indicated below, the suitable jack (Universal Service Order Code connecting arrangement) for this equipment is shown. If applicable, the facility interface codes (FIC) and service order codes (SOC) are shown.
3. An FCC-compliant telephone cord with modular plug is provided with this equipment. This equipment is designed to be connected to the phone network or premises wiring using a compatible modular jack which is Part 68 compliant. See installation instructions for details.
4. The ringer equivalence number (REN) is used to determine the number of devices that may be connected to the phone line. Excessive REN's on the phone line may result in the device not ringing in response to an incoming call. In most, but not all areas, the sum of the REN's should not exceed (5.0). To be certain of the number of devices that may be connected to the line, as determined by the total REN's, contact the local phone company.
5. If this equipment causes harm to the phone network, the phone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the phone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
6. The phone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of the equipment. If this happens, the phone company will provide advance notice in order for you to make necessary modifications in order to maintain uninterrupted service.
7. If trouble is experienced with this equipment (the model of which is indicated below) please contact Multi-Tech Systems, Inc., at the address shown below for details of how to have repairs made. If the equipment is causing harm to the network, the phone company may request that you remove the equipment from the network until the problem is resolved.
8. No repairs are to be made by you. Repairs are to be made only by Multi-Tech Systems or its licensees. Unauthorized repairs void registration and warranty.
9. This equipment should not be used on party lines or coin lines.
10. Manufacturer and device information:

Manufacturer:	Multi-Tech Systems, Inc.
Trade name:	RouteFinderVPN ™
Model Numbers:	RF600VPN, RF660VPN, and RF760VPN
FCC Registration Number:	AU7-USA-25814-M5-E
Ringer Equivalence:	0.3B
Modular Jack:	RJ-11C or RJ-11W
Service Center in U.S.A.:	Multi-Tech Systems Inc. 2205 Woodale Drive Mounds View, MN 55112 (763) 785-3500 Fax (763) 785-9874

Industry Canada for the Modem Operation

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.
Cet appareil numerique de la classe A respecte toutes les exigences du Reglement sur le materiel brouilleur du Canada.

Canadian Limitations Notice for the Modem Operation

Notice: The ringer equivalence number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a phone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the ringer equivalence numbers of all the devices does not exceed 5.
Notice: The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operational and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.
Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Repairs to certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.
Users should ensure for their own protection that the electrical ground connections of the power utility, phone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.
Caution: Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

Appendix J – License Agreements

Multi-Tech Systems, Inc. End User License Agreement (EULA)

IMPORTANT - ***READ BEFORE OPENING THE SOFTWARE PACKAGE***

This is a basic multi-user software license granted by Multi-Tech Systems, Inc., a Minnesota corporation, with its mailing address at 2205 Woodale Drive, Mounds View, MN 55112.

This is a legal agreement between you (either an individual or a single entity) and Multi-Tech Systems, Inc. for the Multi-Tech software product enclosed, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation ("SOFTWARE PRODUCT"). The SOFTWARE PRODUCT also includes any updates and supplements to the original SOFTWARE PRODUCT provided to you by Multi-Tech.

Any software provided along with the SOFTWARE PRODUCT that is associated with a separate end-user license agreement is licensed to you under the terms of that license agreement. By installing, copying, downloading, accessing, or otherwise using the SOFTWARE PRODUCT, you agree to be bound by the terms of that separate end-user license agreement.

This copy of Multi-Tech Systems software is provided only on the condition that you, Customer, agree to the following license agreement. READ THIS LICENSE CAREFULLY. If you do not agree to the terms contained in this license, return the packaged program UNOPENED to the place you obtained it. If you agree to the terms contained in this license, fill out the enclosed Software Registration Card, and return the card by mail. Registration may also be done on Multi-Tech Systems web site at www.multitech.com/register. Opening the packaged program constitutes agreement to be bound by the terms and conditions of this Software License Agreement. Your right to use the software terminates automatically if you violate any part of this software license agreement.

Multi-Tech Software License Agreement

Multi-Tech Systems, Inc. (MTS) agrees to grant and Customer agrees to accept on the following terms and conditions, a non-transferable and non-exclusive license to use the software program(s) delivered with this Agreement.

GRANT OF LICENSE. MTS grants Customer the right to use one copy of the software on a single product (the Licensed System). You may not network the software or otherwise use it on more than one product at the same time.

COPYRIGHT. The software is owned by MTS and is protected by United States copyright laws and international treaty provisions. Therefore, Customer must treat the software like any copyrighted material. Customer may install the software to a single hard disk and keep the original for backup or archival purposes. Customer shall NOT copy, or translate into any language, in whole or in part, any documentation which is provided by MTS in printed form under this Agreement.

OTHER RESTRICTIONS. The software may not be assigned, sublicensed, translated or otherwise transferred by Customer without prior written consent from MTS. Customer may not reverse engineer, decompile, or disassemble the software. Any updates shall be used only on the Licensed System, and shall remain subject to all other terms of this Agreement. Customer agrees not to provide or otherwise make available the software including, but not limited to documentation, programs listings, object code, or source code, in any form, to any person other than Customer and his employees and /or agents, without prior written consent from MTS. Customer acknowledges that the techniques, algorithms, and processes contained in the software are proprietary to MTS and Customer agrees not to use or disclose such information except as necessary to use the software.

Customer shall take reasonable steps consistent with steps taken to protect its own proprietary information to prevent the unauthorized copying or use by third parties of the software or any of the other materials provided under this Agreement. Any previous version of the software must be destroyed or returned to Multi-Tech Systems, Inc. within 90 days of receipt of the software upgrade or update.

LIMITED WARRANTY. MTS warrants that the software will perform substantially in accordance to the product specifications in effect at the time of receipt by Customer. If the MTS software fails to perform accordingly, MTS will optionally repair any defect, or replace it. This warranty is void if the failure has resulted from accident, abuse, or misapplication. A Software Registration Card must be on file at MTS for this warranty to be in effect. In all other respects, the MTS software is provided AS IS. Likewise, any other software provided with MTS software is provided AS IS. THE FOREGOING WARRANTY IS IN LIEU ALL OTHER WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT WILL MTS BE LIABLE FOR CONSEQUENTIAL DAMAGES RESULTING FROM USE OF THE LICENSED PROGRAM, WHETHER AS A RESULT OF MTS NEGLIGENCE OR NOT, EVEN IF MTS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. MTS ALSO DISCLAIMS ANY LIABILITY IN CONTRACT OR OTHERWISE FOR THE DEFECT OR NON-PERFORMANCE OF ANY SEPARATE END-USER LICENSED SOFTWARE PRODUCT INCLUDED WITH MTS' SOFTWARE.

INDEMNIFICATION. MTS will indemnify and defend Customer from any claim that the software infringes on any copyright, trademark, or patent. Customer will indemnify and defend MTS against all other proceedings arising out of Customers use of the software.

GENERAL. If any of the provisions, or portions thereof, of this Agreement are invalid under any applicable statute or rule of law, they are to that extent deemed to be omitted.

This is the complete and exclusive statement of the Agreement between the parties, which supersedes all proposals, oral, written and all other communications between the parties relating to the subject matter of this Agreement. This Agreement may only be amended or modified in writing, signed by authorized representatives of both parties.

This Agreement shall be governed by the laws of the State of Minnesota.

The waiver of one breach or default hereunder shall not constitute the waiver of any subsequent breach or default. Licensee also agrees to the following:

I am not a citizen, national, or resident of, and am not under the control of the government of:

Afghanistan, Cuba, Iran, Iraq, Libya, Montenegro, North Korea, Pakistan, Serbia, Sudan, Syria, nor any other country to which the United States has prohibited export.

I will not download or by any other means export or re-export the Programs, either directly or indirectly, to the above countries, nor to citizens, nationals or residents of the above countries.

I am not listed on the United States Department of Treasury lists of Specially Designated Nationals, Specially Designated Terrorists, and/or Specially Designated Narcotics Traffickers, nor am I listed on the United States Department of Commerce Table of Denial Orders.

I will not download or otherwise export or re-export the Programs, directly or indirectly, to persons on the above mentioned lists.

I will not use the Programs for, and will not allow the Programs to be used for, any purposes prohibited by United States law, including, without limitation, for the development, design, manufacture or production of nuclear, chemical, or biological weapons of mass destruction. Licensee agrees that by purchase and/or use of the Software, s/he hereby accepts and agrees to the terms of this License Agreement.

Multi-User Limited Warranty and License Agreement

The software contained in this package is licensed by Multi-Tech Systems, Inc., to the original end-user purchaser, hereafter referred to as Licensee, of this product for site use. A site is defined as a single business, government, or academic location, such as a building, a floor of a building, a campus, etc., and covers no more than 250 users at that location. A licensee may be a Local Area Network administrator, MIS director, purchasing agent, or other representative who acts on behalf of the users at that single site. This license provides for use of the distribution diskette, other accompanying programs, where applicable, and one copy of the documentation.

The software programs and installation utilities, hereafter referred to as Software, consist of the computer program files included on the original distribution diskette(s) or CD-ROM(s).

Licensee agrees that by purchase and/or use of the Software, s/he hereby accepts and agrees to the terms of this License Agreement. In consideration of mutual covenants contained herein, and other good and valuable considerations, the receipt and sufficiency of which is acknowledged, Multi-Tech Systems, Inc., does hereby grant to the Licensee a non-transferrable and non-exclusive license to use the Software and accompanying documentation under the following terms and conditions:

The software is furnished to the Licensee as the single site representative for execution and use on as many workstations as that single site contains, for up to 250 users inclusively. Software and manuals may be copied, with the inclusion of the Multi-Tech Systems, Inc., copyright notice, for use within that single site. Additional manuals may be ordered from Multi-Tech Systems, Inc., for a nominal charge.

This license covers only the stipulated single site. The Licensee hereby agrees not to provide, or otherwise make available, any portion of this software in any form to any third party without the prior express written approval of Multi-Tech Systems, Inc.

Licensee is hereby informed that this Software contains confidential, proprietary, and valuable trade secrets developed by or licensed to Multi-Tech Systems, Inc., and agrees that sole ownership shall remain with Multi-Tech Systems, Inc.

The Software and documentation are copyrighted. Except as provided herein, the Software and documentation supplied under this agreement may not be copied, reproduced, published, licensed, sub-licensed, distributed, transferred, or made available in any form, in whole or in part, to others without expressed written permission of Multi-Tech Systems, Inc. Copies of the Software may be made to replace worn or deteriorated copies, for archival, or back-up purposes.

Licensee agrees to implement sufficient security measures to protect Multi-Tech Systems, Inc.'s proprietary interests, and not to allow the use, copying, or transfer by any means, other than in accordance with this agreement.

Licensee agrees that any breach of this agreement will be damaging to Multi-Tech Systems, Inc. Licensee agrees that all warranties, implied or otherwise, with regard to this Software, including all warranties of merchantability and fitness for any particular purpose are expressly waived, and no liability shall extend to any damages, including consequential damages, whether known to Multi-Tech Systems, Inc. It is hereby expressly agreed that Licensee's remedy is limited to replacement or refund of the license fee, at the option of Multi-Tech Systems, Inc., for defective distribution media. There is no warranty for misused materials.

If this package contains multiple media formats (e.g., both 3.5" disk(s) and CD-ROM), they are provided only to facilitate use at a single site. Neither this Software, nor its accompanying documentation may be modified or translated without the written permission of Multi-Tech Systems, Inc.

This agreement shall be governed by the laws of the State of Minnesota. The terms and conditions of this agreement shall prevail regardless of the terms of any other submitted by the Licensee. This agreement supersedes any proposal or prior agreement. Licensee further agrees that this License Agreement is the complete and exclusive Statement of Agreement, and supersedes oral, written, or any other communications between Multi-Tech Systems, Inc., and Licensee relating to the subject matter of this agreement. This agreement is not assignable without written permission of an authorized agent of Multi-Tech Systems, Inc.

P/N 87000915 10/01

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

   Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

      These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

      Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

      In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:
   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,
   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.
5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.
6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

   It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

   This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

   Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.
10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.
12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SurfControl URL Filtering End-User Terms

The parties agree that as a condition of the rights and licenses granted by SurfControl under the Agreement, each license agreement to end-users for the Bundle ("End-Users") shall contain, at a minimum, substantially the following terms, allowing reasonable modifications to keep consistent terminology and without materially changing the associated meaning:

SURFCONTROL SOFTWARE LICENSE AGREEMENT

PLEASE READ THIS CAREFULLY BEFORE YOU INSTALL THE SOFTWARE.

LICENSEE'S RIGHT TO USE THIS SOFTWARE IS SUBJECT TO THE TERMS AND CONDITIONS SET OUT IN THIS LICENSE AGREEMENT ("LICENSE"). BY CLICKING ON THE "I ACCEPT" BUTTON AND USING THE SOFTWARE, LICENSEE IS CONSENTING TO BE BOUND BY THIS LICENSE. IF LICENSEE DOES NOT AGREE TO ALL OF THE TERMS AND CONDITIONS OF THIS LICENSE, CLICK ON THE "I DISAGREE" BUTTON AND THE INSTALLATION PROCESS WILL NOT CONTINUE. YOU HEREBY REPRESENT AND WARRANT THAT YOU ARE AUTHORIZED TO BIND THE LICENSEE TO THIS LICENSE.

APPLICABLE MAINTENANCE SERVICES, AS WELL AS NOTIFICATION OF SOFTWARE UPGRADES, ARE PROVIDED ONLY TO LICENSEES WHO COMPLETE THE LICENSE REGISTRATION FORM AT THE TIME THE SOFTWARE IS INSTALLED.

1. DEFINITIONS

1.1. "Activation Key" shall mean the license key which may be provided by SurfControl to Licensee, which allows only a certain number of users to be monitored and/or managed by the Software.

1.2. "Licensee" shall mean the individual or entity whose name appears in the signature block in the License Registration Form.

1.3. "License Registration Form" shall mean the form completed by Licensee at the time of the Software installation, which enables SurfControl to contact Licensee in order to provided warranty services and Maintenance Services, if any.

1.4. "Maintenance Services" means the maintenance and support services provided by SurfControl to Licensee pursuant to Licensee's payment of the applicable maintenance fees, upon the terms set forth on the maintenance terms card enclosed with the Software media, if applicable, or as otherwise made available in writing to Licensee by SurfControl upon Licensee's request.

1.5. "Software" shall mean a copy of the "SurfControl" software program in object code format only, along with the user manual therefore ("Documentation"), that is designed to operate on (i) a single computer called a server, which provides Internet access to end-user devices connected to the server, or (ii) on a single computer which provides Internet access to the user of the computer. The Software may contain technical limitations that limit use of the Software to a certain User Level monitored by the Software, as that number is specified on the applicable Activation Key. The Software may contain then-current versions of the applicable Subscription Lists and such Subscription Lists (and all updates thereto provided pursuant to a Subscription (as defined in Section 8 below), if any) are deemed incorporated into and form a part of the Software.

1.6. "SurfControl" shall mean SurfControl plc (registered in England No. 1566321) Riverside, Mountbatten Way, Congleton, Cheshire, CW12 1DY, England.

1.7. "Subscription Lists" are, if applicable to the Software, certain lists provided periodically on a subscription basis by Licensor for use with the Software, including, without limitation, lists of categorized Internet Web sites, and SPAM and virus detection lists.

1.8. "User Level" shall mean the total number of users being monitored and/or managed by the Software for which Licensee has paid SurfControl the applicable license fees pursuant to this License.

2. GRANT OF LICENSE

In consideration of payment of the license fee, which is a part of the price Licensee paid to use this Software, and Licensee's agreement to abide by the terms and conditions of this License, SurfControl grants to Licensee a non-exclusive, non-transferable right to use this copy of the Software only on a single network, so long as Licensee complies with the terms and conditions of this License. The Software may not allow additional users in excess of the User Level authorized by the Activation Key. Licensee may install the Software on any one server (or more servers if the appropriate additional fees have been paid) within Licensee's network. Installation on a network server for the sole purpose of internal distribution of the Software shall not constitute a "use" for which a separate license is required, provided Licensee has obtained a license and paid the fees for each user who is being monitored and/or managed by the Software. Licensee may make one (1) copy of the Software solely for back-up purposes. Licensee must reproduce and include the copyright, trademark and proprietary notices on the back-up copy. Licensee receives only the rights expressly granted to it in this License and does not receive any implied rights. SurfControl reserves all rights not expressly granted to Licensee.

3. OWNERSHIP

This License is not a sale of the Software or any copy of the Software. An express condition of this License is that SurfControl and its licensors retain all worldwide ownership of and rights, title and interest in and to the Software, and all copies and portions thereof, including without limitation, all copyrights, moral rights, trademark rights, trade secret rights and other proprietary rights therein and thereto, regardless of the form or media in or on which the Software or copies may exist. All logos and product names appearing on or in connection with it, and any other materials provided with it, if any, are proprietary to SurfControl or its licensors and/or suppliers. Licensee agrees never to remove any proprietary notices or product identification labels from the Software and any accompanying media, if applicable.

4. COPY RESTRICTION

This Software is protected by copyright laws around the world. Unauthorized copying of the Software, including Software which has been modified, merged, or included with other software, is expressly forbidden. Licensee may be held legally responsible for any copyright infringement which is caused or encouraged by Licensee's failure to abide by the terms and conditions of this License.

5. USE RESTRICTIONS; AUDIT

Licensee must have a reasonable mechanism in place to ensure that Licensee's use of the Software does not exceed the User Level. Licensee may only add additional users to the User Level upon the payment of additional license fees to SurfControl. Upon notice, SurfControl may audit Licensee's use of the Software, at SurfControl's option, at Licensee's premises or by remote means, including without limitation, by telephone interviews and facsimile transmission of relevant documents. All audits will be conducted during Licensee's normal business hours, to determine Licensee's compliance with the terms of this License, including, without limitation, User Level restrictions. SurfControl shall send an invoice to Licensee for any additional users in excess of the User Level that SurfControl may discover during any audit, and Licensee shall pay the amount stated in the invoice within thirty (30) days of receipt of the invoice. This License shall automatically terminate if Licensee does not pay the invoice during that time.

Licensee may not disclose, modify, adapt, translate, reverse engineer, disassemble, decompile or create derivative works from the Software or any portion of the Software, including, without limitation, any databases that comprise the Software, the organization of such databases

and/or the Subscription Lists, if any. Licensee may not permit third parties to benefit from the use or functionality of the Software via a service bureau or other arrangement. Licensee may not copy the Software except as expressly permitted in Section 2 above.

Licensee agrees that the use of the Software may be restricted by applicable laws and regulations, including without limitation, privacy laws. Licensee represents and warrants that Licensee's use of the Software shall be in compliance with any applicable laws and regulations, including without limitation, privacy laws, and that SurfControl shall have no duty to and shall not investigate Licensee's use of the Software or right to use the Software. Licensee agrees to indemnify SurfControl against any claims that Licensee's use of the Software violates the rights of any third party or any applicable laws and/or regulations of any jurisdictions, except to the extent the Software infringes any patent, copyright or trade secret of a third party.

6. TRANSFER RESTRICTIONS

This Software is licensed only to Licensee and may not be transferred to anyone without the prior written consent of SurfControl. Any authorized transferee of the Software shall agree in writing to be bound by the terms and conditions of this License. In no event may Licensee transfer, assign, rent, lease, loan, time-share, sublicense, sell or otherwise dispose of the Software on a temporary or permanent basis except as expressly provided herein. This License shall benefit SurfControl and its successors and assigns.

7. TERMINATION

This License is effective on the date Licensee installs the Software and shall continue until terminated. This License will terminate automatically without notice from SurfControl if Licensee fails to comply with any provision of this License or if Licensee becomes bankrupt, goes into liquidation, suffers or is the subject of any winding-up petition, makes an arrangement with Licensee's creditors, has an administrator or receiver appointed or suffers or files any similar action in consequence of debt. Licensee may terminate this License by destroying all copies of the Software. Upon termination Licensee shall destroy all copies of the Software. Upon termination there will be no refund of any monies or other consideration paid by Licensee. The following Sections shall survive termination of this License for any reason: 1, 3, 7, 9, 10, 11, 13, 14, 15 and 16.

8. MAINTENANCE AND UPGRADE POLICY

SurfControl will provide maintenance and support for the Software solely pursuant to Licensee's purchase of Maintenance Services. SurfControl may create, from time to time, upgraded versions of the Software. SurfControl will only make such upgrades available to (a) Licensee and authorized transferees, if any, who have completed the License Registration Form during the Software installation process and paid any applicable upgrade fees or (b) Licensee pursuant to the Maintenance Services, if applicable.

This License does not provide Licensee with any right to any upgrades or future versions of the Subscription Lists. Licensee may have rights to receive updates to certain Subscription Lists made generally available by SurfControl during the applicable term of Licensee's subscription to such Subscription Lists (the "Subscription"), if any.

9. CHOICE OF LAW

This License shall be governed and construed in accordance with the laws of the United States of America and the State of California as applied to agreements entered into and to be performed entirely within California between California residents. This License shall be deemed to have been made and entered into in Santa Clara, California. The parties hereby submit to the non-exclusive jurisdiction of, and waive any venue objections against, the United States District Court for the Northern District of California, San Jose Branch and the Superior and Municipal Courts of the State of California, Santa Clara County, in any litigation arising out of or in connection with the License. The parties expressly disclaim application of the United Nations Convention on Contracts for the International Sale of Goods.

10. LIMITED WARRANTY AND DISCLAIMER OF WARRANTY

SURFCONTROL WARRANTS THAT ON THE DATE THE LICENSE REGISTRATION FORM IS COMPLETED AND THE SOFTWARE IS INSTALLED, THE SOFTWARE WHEN USED PROPERLY, WILL SUBSTANTIALLY CONFORM WITH THE FUNCTIONS AND FACILITIES DESCRIBED IN THE DOCUMENTATION AND IN ANY WRITTEN OPERATION GUIDE TO THE SOFTWARE GENERALLY MADE AVAILABLE BY SURFCONTROL. THIS WARRANTY SHALL ONLY BE EFFECTIVE IF THE LICENSE REGISTRATION FORM IS COMPLETED AND SUBMITTED AT THE TIME THE SOFTWARE IS INSTALLED. THE FOREGOING WARRANTY IS VOID, HOWEVER, IF FAILURE OF THE SOFTWARE HAS RESULTED FROM ACCIDENT, ABUSE, OR MISAPPLICATION.

LICENSEE'S SOLE AND EXCLUSIVE REMEDY AND SURFCONTROL'S SOLE AND EXCLUSIVE LIABILITY FOR FAILURE OF THE SOFTWARE TO MEET THE FOREGOING WARRANTY WILL BE, AT SURFCONTROL'S OPTION, TO EITHER REPAIR OR REPLACE THE DEFECTIVE SOFTWARE OR MEDIA, IF APPLICABLE. THIS REMEDY IS SUBJECT TO LICENSEE'S FULL COMPLIANCE WITH THE TERMS AND CONDITIONS OF THIS LICENSE. LICENSEE MUST NOTIFY SURFCONTROL WITHIN THIRTY (30) DAYS AFTER INSTALLING THE SOFTWARE OF ANY DEFECT IN ORDER TO RECEIVE THE REMEDY STATED ABOVE. ANY REPLACEMENT MEDIA WILL BE WARRANTED FOR THE REMAINDER OF THE ORIGINAL WARRANTY PERIOD. OUTSIDE THE UNITED STATES, THIS REMEDY IS NOT AVAILABLE TO THE EXTENT SURFCONTROL AND/OR ITS LICENSORS ARE SUBJECT TO RESTRICTIONS UNDER UNITED STATES EXPORT CONTROL LAWS AND REGULATIONS.

EXCEPT FOR THE WARRANTIES STATED IN THIS SECTION 10, THE SOFTWARE, INCLUDING, WITHOUT LIMITATION, THE SUBSCRIPTION LISTS, IF APPLICABLE, AND ANY DOCUMENTATION, IS PROVIDED "AS IS" WITHOUT ADDITIONAL WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. FURTHER, SURFCONTROL DOES NOT WARRANT, GUARANTEE OR MAKE ANY REPRESENTATIONS REGARDING THE USE, OR THE RESULTS OF USE, OF THE SOFTWARE, SUBSCRIPTION LISTS OR WRITTEN MATERIALS PROVIDED BY SURFCONTROL IN TERMS OF CORRECTNESS, ACCURACY, COMPLETENESS, RELIABILITY, CURRENTNESS, OR OTHERWISE. SURFCONTROL SPECIFICALLY DOES NOT WARRANT THAT THE SOFTWARE OR SUBSCRIPTION LISTS WILL PREVENT ACCESS TO OFFENSIVE OR OBSCENE MATERIAL, OR SPAM OR VIRUSES FROM AFFECTING LICENSEE'S COMPUTER NETWORK. LICENSEE ACKNOWLEDGES THAT IT IS LICENSEE'S SOLE RESPONSIBILITY TO MAINTAIN SUCH WORKPLACE POLICIES AND PROCEDURES TO ENSURE AN ENVIRONMENT FREE OF HOSTILITY AND SEXUAL HARASSMENT. LICENSEE ASSUMES THE ENTIRE RISK AS TO THE RESULTS AND PERFORMANCE OF THE SOFTWARE AND SUBSCRIPTION LISTS, IF ANY.

SURFCONTROL MAKES NO OTHER WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE AVAILABILITY OF SURFCONTROL'S SITE ON THE WORLDWIDE WEB, OR THE IMPLIED WARRANTIES OF NON-INFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. No oral or written information or advice given by SurfControl, its dealers, distributors, agents or employees shall create a warranty or in any way increase the scope of this warranty and Licensee may not rely on any such information or advice.

11. LIMITATION OF LIABILITY

IN NO EVENT WILL SURFCONTROL OR ITS AFFILIATES, SUPPLIERS, AND/OR LICENSORS BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, ECONOMIC, COVER, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, SUBSCRIPTION LISTS, USER DOCUMENTATION, OR RELATED TECHNICAL SUPPORT, INCLUDING, WITHOUT LIMITATION, DAMAGES OR COSTS RELATING TO THE LOSS OF PROFITS, BUSINESS, GOODWILL, DATA, OR COMPUTER PROGRAMS, OR ANY DAMAGES RELATED TO ACCESS OR EXPOSURE TO OFFENSIVE OR OBSCENE MATERIAL, SPAM AND/OR VIRUSES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL THE TOTAL LIABILITY OF SURFCONTROL AND ITS AFFILIATES, SUPPLIERS, AND/OR LICENSORS EXCEED THE AMOUNT PAID BY LICENSEE FOR THE SOFTWARE.

THESE LIMITATIONS APPLY TO ALL CAUSES OF ACTION IN THE AGGREGATE, INCLUDING WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, SURFCONTROL'S NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION AND OTHER TORTS.

Licensee acknowledges that the allocation of risk in this License reflects the price paid for the Software and also the fact that it is not within SurfControl's control how or for what purposes the Software is used.

THE SECTIONS ON LIMITATION OF LIABILITY, WARRANTIES AND DISCLAIMER OF WARRANTIES ALLOCATE THE RISKS OF THIS LICENSE BETWEEN THE PARTIES. THIS ALLOCATION IS REFLECTED IN THE PRICING OF THE SOFTWARE AND IS AN ESSENTIAL ELEMENT OF THE BASIS OF THE BARGAIN BETWEEN THE PARTIES AND SHALL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF THIS LICENSE OR ANY REMEDY HEREUNDER.

12. U.S. GOVERNMENT RESTRICTED RIGHTS

If Licensee is an agency of the U.S. Government, then the Software and related documentation provided shall be "commercial computer software" and "commercial computer software documentation," respectively, as such terms are used in 48 C.F.R. 12.212 of the Federal Acquisition Regulations ("FAR") and its successors and 48 C.F.R. 227.7202 of the Department of Defense FAR Supplement ("DFARS") and its successors. In accordance with FAR 12.212 or DFARS 227.7202, as applicable, the Software and related documentation are provided to all U.S. Government end-users with only those rights set forth in this License.

13. INDEMNITY

Licensee shall indemnify SurfControl, its employees and agents from and against all costs, claims, demands, expenses, fines, penalties and liabilities whatsoever which may be made against, sustained, paid or incurred by SurfControl, its employees or agents as a direct or indirect result of Licensee's breach of contract, negligence, breach
of statutory duty or other act or omission.

14. IMPORT/EXPORT

Licensee acknowledges that the Software may be governed by laws, rules and/or regulations, including, without limitation, the laws and regulations of the United States, which restrict the import, export and re-export of certain software, technical data and other materials. Licensee agrees that it will not directly or indirectly, violate any local, state or federal law or regulation of the country or countries in which Licensee uses the Software, or the export laws of any country which may regulate the import or export of the Software.

15. HIGH RISK ACTIVITIES

The Software is not fault-tolerant and is not designed or intended for use in hazardous environments requiring fail-safe performance, including without limitation, in the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, weapons systems, direct life-support machines, or any other application in which the failure of the Software could lead directly to death, personal injury, or severe physical or property damage (collectively, "High Risk Activities"). SurfControl expressly disclaims any express or implied warranty of fitness for High Risk Activities.

16. MISCELLANEOUS

Licensee acknowledges and agrees that SurfControl may use Licensee's name in SurfControl's marketing materials and/or a list of SurfControl's customers.

Licensee acknowledges that it has read this License, understands it and agrees to be bound by its terms and conditions. Licensee also agrees that the License is the complete and exclusive statement of agreement between the parties and supersedes all proposals or prior or contemporaneous oral or written agreements, and any other communications between the parties relating to the subject matter of the License. It is the intent of the parties that this License will prevail over the terms and conditions of any purchase order, acknowledgment form or other instrument. Any terms and conditions of any purchase order which are in addition to or inconsistent with the terms and conditions of this License will be deemed stricken from such purchase order, notwithstanding acknowledgment or acceptance of such purchase order.

No waiver of any right under this License shall be deemed effective unless contained in writing and signed by a duly authorized representative of SurfControl, and no waiver of any past or present right arising from any breach or failure to perform shall be deemed to be a waiver of any future right arising under this License. If any provision in this License is invalid or unenforceable, that provision shall be reformed to the maximum extent allowed by law to reflect the same economic effect as the invalid or unenforceable provision, and the other provisions of this License shall remain in full force and effect.

Except for the obligation to pay license fees, a party's performance under this License is excused if that party is unable to perform under this License due to an event beyond its reasonable control, including without limitation, natural disasters, labor unrest, government restrictions, and the like. Licensee shall be responsible for payment of all taxes and duties due pursuant to this License. The section headings appearing in this License are for the convenience of the parties and do not define or limit the scope or intent of such sections. No modification of this License shall be binding unless it is in writing and signed by authorized representatives of both parties. The English language will be the controlling language of this License. All communications and notices given pursuant to this License will be in the English language. Should you have any questions concerning this License, please contact SurfControl in writing.

Kaspersky Standard End User License Agreement.

Standard End User License Agreement

NOTICE TO ALL USERS: CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT ("AGREEMENT"), FOR THE LICENSE OF SPECIFIED SOFTWARE ("SOFTWARE") PRODUCED BY KASPERSKY LAB. ("KASPERSKY LAB").

IF YOU HAVE PURCHASED THIS SOFTWARE VIA INTERNET BY CLICKING THE ACCEPT BUTTON, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) CONSENT TO BE BOUND BY AND BECOME A PARTY TO THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, CLICK THE BUTTON THAT INDICATES THAT YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT AND DO NOT INSTALL THE SOFTWARE.

IF YOU HAVE PURCHASED THIS SOFTWARE ON A PHYSICAL MEDIUM, HAVING BROKEN THE CD'S SLEEVE, YOU (EITHER AN INDIVIDUAL OR A SINGLE ENTITY) ARE CONSENTING TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THIS AGREEMENT DO NOT BREAK THE CD's SLEEVE ,DOWNLOAD, INSTALL OR USE THIS SOFTWARE. YOU MAY RETURN THIS SOFTWARE FOR A FULL REFUND. YOUR RIGHT TO RETURN AND REFUND EXPIRES 30 DAYS AFTER PURCHASE FROM AN AUTHORISED KASPERSKY LAB DISTRIBUTOR OR RESELLER. THE RIGHT TO RETURN AND REFUND EXTENDS ONLY TO THE ORIGINAL PURCHASER.

All references to "Software" herein shall be deemed to include the software activation key ("Key Identification File") with which you will be provided by Kaspersky Lab as part of the Software.

License Grant. Subject to the payment of the applicable license fees, and subject to the terms and conditions of this Agreement, Kaspersky Lab hereby grants to you a non-exclusive, non-transferable right to use one copy of the specified version of the Software and the accompanying documentation (the "Documentation") for the term of this Agreement solely for your own internal business purposes. You may install one copy of the Software on one computer, workstation, personal digital assistant, or other electronic device for which the Software was designed (each, a "Client Device"). If the Software is licensed as a suite or bundle with more than one specified Software produce, this license applies to all such specified Software products, subject to any restrictions or usage terms specified on the applicable price list or product packaging that apply to any of such Software products individually.

Use. The Software is licensed as a single product; it may not be used on more than one Client Device or by more than one user at a time, except as set forth in this Section.

The Software is "in use" on a Client Device when it is loaded into the temporary memory (i.e., random-access memory or RAM) or installed into the permanent memory (e.g., hard disk, CD-ROM, or other storage device) of that Client Device. This license authorizes you to make only as many back-up copies of the Software as are necessary for its lawful use and solely for back-up purposes, provided that all such copies contain all of the Software's proprietary notices. You will maintain records of the number and location of all copies of the Software and Documentation and will take all reasonable precautions to protect the Software from unauthorized copying or use.

If you sell the Client Device on which the Software is installed, you will ensure that all copies of the Software have been previously deleted.

You shall not decompile, reverse engineer, disassemble or otherwise reduce any party of this Software to human readable form nor permit any third party to do so. The interface information necessary to achieve interoperability of the Software with independently created computer programs will be provided by Kaspersky Lab on request on payment of its reasonable costs and expenses for procuring and supplying such information. In the event Kaspersky Lab notifies you that it does not intend to make such information available for any reason, including (without limitation) costs, you shall be permitted to take such steps to achieve interoperability provided that you may only reverse engineer or decompile to the extent permitted by law.

You shall not, nor permit any third party to copy (other than as expressly permitted herein), make error corrections to or otherwise modify, adapt or translate the Software nor create derivative works of the Software.

You shall not rent, lease or lend the Software to any other person, nor transfer or sub-license your license rights to any other person.

Server-Mode Use. You may use the Software on a Client Device or on or as a server ("Server") within a multi-user or networked environment ("Server-Mode") only if such use is permitted in the applicable price list or product packaging for the Software. A separate license is required for each Client Device or "seat" that may connect to the Server at any time, regardless of whether such licensed Client Devices or seats are concurrently connected to or actually accessing or using the Software. Use of software or hardware that reduces the number of Client Devices or seats directly accessing or utilizing the Software (e.g., "multiplexing" or "pooling" software or hardware) does not reduce the number of licenses required (i.e., the required number of licenses would equal the number of distinct inputs to the multiplexing or pooling software or hardware "front end"). If the number of Client Devices or seats that can connect to the Software can exceed the number of licenses you have obtained, then you much have a reasonable mechanism in place to ensure that your use of the Software does not exceed the use limits specified for the license you have obtained. This license authorizes you to make or download such copies of the Documentation for each Client Device or seat that is licensed as are necessary for its lawful use, provided that each such copy contains all of the Documentation proprietary notices.

Volume Licenses. If the Software is licensed with volume license terms specified in the applicable product invoicing or packaging for the Software, you may make, use or install as many additional copies of the Software on the number of Client Devices as the volume license terms specify. You must have reasonable mechanisms in place to ensure that the number of Client Devices on which the Software has been installed does not exceed the number of licenses you have obtained. This license authorizes you to make or download one copy of the Documentation for each additional copy authorized by the volume license, provided that each such copy contains all of the Document's proprietary notices.

Term. This Agreement is effective for [one (1)] year unless and until earlier terminated as set forth herein. This Agreement will terminate automatically if you fail to comply with any of the conditions, limitations or other requirements described herein. Upon any termination or expiration of this Agreement, you must immediately destroy all copies of the Software and the Documentation. You may terminate this Agreement at any point by destroying all copies of the Software and the Documentation.

Support

(i) Kaspersky Lab will provide you with the support services ("Support Services") as defined below for a period of one year on:
   (a) payment of its then current support charge; and
   (b) successful completion of the Support Services Subscription Form as provided to you with this Agreement or as available on the Kaspersky Lab Web site, which will require you to produce the Key Identification File which will have been provided to you by Kaspersky Lab with this Agreement. It shall be in the absolute discretion of Kaspersky Lab whether or not you have satisfied this condition for the provision of Support Services.

(ii) Support Services will terminate unless renewed annually by payment of the then current annual support charge and by successful completion of the Support Services Subscription Form again.

(iii) By completion of the Support Services Subscription Form you consent to the terms of the Kaspersky Lab Privacy Policy which is attached to this Agreement, and you explicitly consent to the transfer of data to other countries outside your own as set out in the Privacy Policy.

(iv) "Support Services" means

Weekly updates of antivirus databases;

Free software updates, including version upgrades;

Extended technical support via E-mail and hot phone-line provided by Vendor and/or Reseller;

Virus detection and curing updates in 24-hours period.

Ownership Rights. The Software is protected by copyright laws. Kaspersky Lab and its suppliers own and retain all right, title and interest in and to the Software, including all copyrights, patents, trademarks and other intellectual property rights therein. Your possession, installation, or use of the Software does not transfer to you any title to the intellectual property in the Software, and you will not acquire any rights to the Software except as expressly set forth in this Agreement.

Confidentiality. You agree that the Software and the Documentation, including the specific design and structure of individual programs and the Key Identification File constitute confidential proprietary information of Kaspersky Lab. You shall not disclose, provide or otherwise make available such confidential information in any form to any third party without the prior written consent of Kaspersky Lab. You shall implement reasonable security measures to protect such confidential information, but without limitation to the foregoing shall use best endeavors to maintain the security of the Key Identification File.

Limited Warranty

Kaspersky Lab warrants that for [90] days from first download or installation the Software will perform substantially in accordance with the functionality described in the Documentation when operated properly and in the manner specified in the Documentation.

You accept all responsibility for the selection of this Software to meet your requirements. Kaspersky Lab does not warrant that the Software and/or the Documentation will be suitable for such requirements nor that any use will be uninterrupted and error free; Kaspersky Lab does not warrant that this Software identifies all known viruses, nor that the Software will not occasionally erroneously report a virus in a title not infected by that virus;

Your sole remedy and the entire liability of Kaspersky Lab for breach of the warranty at paragraph (i) will be at Kaspersky Lab option, to repair, replace or refund of the Software if reported to Kaspersky Lab or its designee during the warranty period. You shall provide all information as may be reasonably necessary to assist the Supplier in resolving the defective item;

The warranty in (i) shall not apply if you (a) make or cause to be made any modifications to this Software without the consent of Kaspersky Lab, (b) use the Software in a manner for which it was not intended or (c) use the Software other than as permitted under this Agreement;

The warranties and conditions stated in this Agreement are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Software or the Documentation which might but for this paragraph (v) have effect between the Kaspersky Lab and your or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

Limitation of Liability

Nothing in this Agreement shall exclude or limit Kaspersky Lab' liability for (i) the tort of deceit, (ii) death or personal injury caused by its breach of a common law duty of care or any negligent breach of a term of this Agreement, (iii) any breach of the obligations implied by s.12 Sale of Goods Act 1979 or s.2 Supply of Goods and Services Act 1982 or (iv) any liability which cannot be excluded by law.

Subject to paragraph (i), the Supplier shall have no liability (whether in contract, tort, restitution or otherwise) for any of the following losses or damage (whether such losses or damage were foreseen, foreseeable, known or otherwise):

Loss of revenue;

Loss of actual or anticipated profits (including for loss of profits on contracts);

Loss of the use of money;

Loss of anticipated savings;

Loss of business;

Loss of opportunity;

Loss of goodwill;

Loss of reputation;

Loss of, damage to or corruption of data; or

Any indirect or consequential loss or damage howsoever caused (including, for the avoidance of doubt, where such loss or damage is of the type specified in paragraph (ii), (a) to (ii), (i).

Subject to paragraph (i), the Kaspersky Lab liability (whether in contract, tort, restitution or otherwise) arising out of or in connection with the supply of the Software shall in no circumstances exceed a sum equal to the amount equally paid by you for the Software.

The construction and interpretation of this Agreement shall be governed in accordance with the laws of England and Wales. The parties hereby submit to the jurisdiction of the courts of England and Wales save that Kaspersky Lab as claimant shall be entitled to initiate proceedings in any court of competent jurisdiction.

(i) This Agreement contains the entire understanding of the parties with respect to the subject matter hereof and supersedes all and any prior understandings, undertakings and promises between you and Kaspersky Lab, whether oral or in writing, which have been given or may be implied from anything written or said in negotiations between us or our representatives prior to this Agreement and all prior agreements between the parties relating to the matters aforesaid shall cease to have effect as from the Effective Date. Save as provided in paragraphs (ii) - (iii), you shall not have any remedy in respect of an untrue statement made to you upon which you relied in entering into this Agreement ("Misrepresentation") and Kaspersky Lab shall not have any liability to the other than pursuant to the express terms of this Agreement.

(ii) Nothing in this Agreement shall exclude or limit Kaspersky Lab' liability for any Misrepresentation made by it knowing that it was untrue.

(iii) The liability of Kaspersky Lab for Misrepresentation as to a fundamental matter, including a matter fundamental to the maker's ability to perform its obligations under this Agreement, shall be subject to the limitation of liability set out in paragraph 7(iii).

Appendix K – Waste Electrical and Electronic Equipment Directive (WEEE)

Waste Electrical and Electronic Equipment (WEEE) Directive

The WEEE directive places an obligation on manufacturers, distributors and retailers to take-back electronic products at the end of their useful life. A sister Directive, ROHS (Restriction of Hazardous Substances), complements the WEEE Directive by banning the presence of specific hazardous substances in the products at the design phase. The WEEE Directive covers all Multi-Tech products being sold into the EU as of August 13, 2005. Manufacturers, distributors and retailers are obliged to finance the costs of recovery from municipal collection points, reuse, and recycling of specified percentages per the WEEE requirements.

Instructions for Disposal of WEEE by Users in the European Union

The symbol shown below is on the product or on its packaging which indicates that this product must not be disposed of with other waste. Instead, it is the user's responsibility to dispose of the user's waste equipment by handing it over to a designated collection point for the recycling of electrical and electronic waste equipment. The separate collection and recycling of waste equipment at the time of disposal will help to conserve natural resources and ensure that it is recycled in a manner that protects human health and the environment. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the seller from whom you purchased the product.

06/27/2005

Glossary

*** (Asterisk character)** – The 'wildcard' character, used to signify "all within this group or function" (e.g., use ***** to specify all domain names). A special symbol that stands for one or more characters. Many operating systems and applications support wildcards for identifying files and directories. This lets you select multiple files with a single specification. For example, in DOS and Windows, the asterisk (*) is a wild card that stands for any combination of letters.

: (colon character) – The character used by the RouteFinder **Web Admin** software for a port range. For example, to enter the S-Port/Client source port number as a port range, enter 1024:64000.

, (comma character) – The character used by the RouteFinder **Web Admin** software for a list of port numbers. For example, to enter the S-Port/Client source port number as a list of port numbers, enter 25, 80, 110.

- (dash character) – An acceptable RouteFinder WebAdmin entry field character. For example, from **VPN > IPSec > Add an IKE connection > Secret)** you can enter a shared **Secret** using alphanumeric characters, the dash (**-**) or the space or underline (**_**) characters.

_ (space or underscore character) – An acceptable RouteFinder WebAdmin entry field character. For example, from **VPN > IPSec > Secret)** you can enter a shared **Secret** using alphanumeric characters, the dash (**-**) or the space or underline (**_**) characters.

3DES (Triple Data Encryption Standard) – The 3DES encryption algorithm combines three uses of single DES with two keys, making the key size 112 bits. With the increase in size, 3DES is much more secure than DES, but 3DES runs slower than DES. The RouteFinder supports up to 256 tunnels with 3DES encryption throughput of 15M bps (e.g., 3DES can be configured in WebAdmin from **VPN > IPSEC**).
The RouteFinder uses 3DES as an encryption algorithm and not simple DES (Data Encryption Standard) because simple DES is generally known to be insecure and out of date.
The RouteFinder default selection is **3 des-md5-96** .

AES (Advanced Encryption Standard) – The U.S. government standard for data encryption.
Rijndael was chosen as the U.S. government encryption standard to protect sensitive data and to spur the digital economy, replacing DES. The algorithms used by the Rijndael AES have since been adopted by businesses and organizations worldwide.

Alias – A name, usually short, easy to remember is translated into another name, usually long and difficult to remember.

Anonymous FTP – Anonymous FTP allows a user to retrieve documents, files, programs, and other archived data from anywhere in the Internet without having to establish a user ID and password. By using the special user ID of "anonymous" the network user will bypass local security checks and will have access to publicly accessible files on the remote system.

ARP (Address Resolution Protocol) – An IETF standard that allows an IP node to determine the hardware (datalink) address of a neighboring node. ARP provides a method of converting Protocol Addresses (e.g., IP addresses) to Local Network Addresses (e.g., Ethernet addresses). ARP exists as a low-level protocol within the TCP/IP suite and is used to "map" IP addresses to Ethernet (or other) addresses (i.e., ARP provides the physical address when only the logical address is known).

Attack – An attempt at breaking part or all of a cryptosystem; can be either a successful or unsuccessful attempt. Many types of attacks can occur (e.g., algebraic attack, birthday attack, brute force attack, chosen ciphertext attack, chosen plain text attack, known plain text attack, linear cryptanalysis, middleperson attack).

Authentication – The action of verifying information such as identity, ownership or authorization.
Authentication is a security process where user access is allowed only if user authentication verifies the identity of the user requesting access to network resources. Authentication is one of the functions of IPSec. Authentication establishes the integrity of a data stream, ensures that it is not tampered with in transit, and confirms the data stream's origin. Authentication establishes the legitimacy of users and defines the allowed parameters of the session they establish.

Authentication Header (AH) – A provision of IPSec that adds a digital signature to an IP packet. The digital signature is created through a key-controlled "hashing" of each packet, providing user authentication, and system integrity.

Broadcast – The address that a computer refers to if it wants to address all the computers of a network. Example: for a network with the IP address 212.6.145.0 and a net mask 225.225.225.240, a broadcast would be the address 212.6.145.15.

CSS (Cascading Style Sheets) – HTML was intended to mark up only a Web page's structure, but not its on-screen display characteristics. For Web page appearances, the World Wide Web Consortium (W3C) developed a complementary markup system called Cascading Style Sheets (CSS) to make it easier to define a page's appearance without affecting its HTML structure. HTML can be frustrating when trying to control the appearance of a Web page and its contents. Style sheets work like templates: you define the style for a particular HTML element once, and then use it over and over on any number of Web pages. To change how an element looks, you just change the style; the element automatically changes wherever it appears. (Before CSS, you had to change the element individually, each time it appeared.) Style sheets let Web designers more quickly create consistent pages and more consistent web sites.
Browsers began supporting the first CSS Specification, Cascading Style Sheets, Level 1 (CSS1), in versions 3.0 of Opera and Microsoft Internet Explorer and in version 4.0 of Netscape Navigator. The 4.0 and later versions of all three browsers also support properties from the newer Cascading Style Sheets, Level 2 (CSS2) specification, which let you specify elements' visibilities, their precise positions on the page, and how they overlap each other.

Certificate – A cryptographically signed object that contains an identity and a public key associated with the identity. Public key certificates are digital stamps of approval for electronic security. The three main characteristics of certificates are 1) provide identification of the web site and the owner, 2) contain the public key to be used to encrypt and decrypt messages between parties, and 3) provide a digital signature from the trusted organization that issued the certificate, as well as when the certificate expires.

Certificate Authority – The issuer of a certificate is the Certificate Authority (CA). The CA is the party that digitally signs a certificate and ensures its validity. There are two types of CAs, private and public. Private CAs issue certificates for use in private networks where they can validate the certificate. Public CAs issues certificates for servers that belong to the general public. A Public CA must meet certain requirements before they are added as a root authority to a browser. Since this is a controlled process, all public CA must be registered to issue certificates.

Certificate Revocation List – A log of certificates that have been revoked before their expiration date.

Cipher – An encryption/decryption algorithm.

Ciphertext – Encrypted data.

Client-Server Model – A common way to describe the paradigm of many network protocols. Examples include the name-server/name-resolver relationship in DNS and the file-server/file-client relationship in NFS.

CHAP (Challenge Handshake Authentication Protocol) – An IETF standard for authentication using PPP which uses a "random Challenge", with a cryptographically hashed "Response" which depends on the Challenge and a secret key.

Client – A client is a program that communicates with a server via a network, so as to use the service provided by that server. Example: Netscape is a www client, with the help of which one can call up information from a www server.

Client-Server Principle – Applications based on the client-server principle use a client program (client) at the user-end that exchanges information with a server on the network. Usually the server is responsible for the data keeping, while the client takes over the presentation of this information and the interaction with the user. For this, the server and the client employ an exactly defined protocol. All the important applications in the Internet (e.g. www, FTP, news) are based on the client-server principle.

CMP (Certificate Management Protocol) – A protocol defining the online interactions between the end entities and the certification authority in PKI. It is written by PKIX working group of IETF and is specified in document RFC 2510.

Compromise – The unintended disclosure or discovery of a cryptographic key or secret.

CRL – Certificate Revocation List.

Cryptography – The art and science of using mathematics to secure information and create a high degree of trust in the networking realm. See also public key, secret key.

CSR (Certificate Signing Request) – The form used to obtain a certificate from a CA. A CSR generates a formatted certification. This request is located on the web site of all certificate authorities. Another way to generate a CSR is to use a utility such as Microsoft IIS or OpenSSL.

Datagram – The unit of transmission at the ISO Network layer (such as IP). A datagram may be encapsulated in one or more packets passed to the data link layer. A datagram is a self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.

CefaultRoute – A routing table entry that is used to direct packets addressed to networks not explicitly listed in the routing table.

DES (Data Encryption Standard) – A secret key encryption scheme; contrast with “public key”. DES is an NIST standard for a secret key cryptography method that uses a 56-bit key.

Destination Port Number ZZZZ – All the traffic going through the firewall is part of a connection. A connection consists of the pair of IP addresses that are talking to each other, as well a pair of port numbers. The destination port number often indicates the type of service being connected to. When a firewall blocks a connection, it will save the destination port number to its logfile.
Port numbers are divided into three ranges:

- The Well-Known Ports are those from 0 through 1023. These are tightly bound to services, and usually traffic on this port clearly indicates the protocol for that service. For example, port 80 virtually always indicates HTTP traffic.
- The Registered Ports are those from 1024 through 49151. These are loosely bound to services, which means that while there are numerous services "bound" to these ports, these ports are likewise used for many other purposes. For example, most systems start handing out dynamic ports starting around 1024.
- The Dynamic and/or Private Ports are those from 49152 through 65535. In theory, no service should be assigned to these ports.

DHCP (Dynamic Host Configuration Protocol) – An IETF standard for dynamically allocating and managing a pool of IP addresses, allowing a smaller number of addresses to serve a much larger number of users.

Digital Signature – The encryption of a message digest with a private key. Digital signatures are based on public-key cryptography, which was first introduced by Whitfield Diffie and Martin Hellman of Stanford University in 1976. Until 1976 there was only conventional cryptography, which uses the same key to both scramble (encrypt) and unscramble (decrypt) information. Public key cryptography is based on two keys, a private key and a public key.
Where conventional cryptography is a one-key system for both locking (encrypting) and unlocking (decrypting) a message, public key cryptography uses different keys for locking and unlocking.
In public-key systems, one key can be kept private while the other key is made public. Knowing the public key does not reveal the private key.

DMZ (De-militarized Zone) – A special LAN on the public network side of a firewall to allow a single WAN router to support both private (VPN) and public access to resources. A DMZ allows a single WAN router to support both private (VPN) and public access to resources. Using a DMZ allows one IP Address (computer) to be exposed to the Internet. Some applications require multiple TCP/IP ports to be open. A DMZ allows just one computer to be exposed for that purpose. It is recommended that you set your computer with a static IP if you want to use DMZ.

DNAT (Dynamic NAT) – Used to operate a private network behind a firewall and make network services that only run there available to the Internet.
The use of private IP addresses in combination with Network Address Translation (NAT) in the form of Masquerading, Source NAT (SNAT), and Destination NAT (DNAT) allows a whole network to hide behind one or a few IP addresses preventing the identification of your network topology from the outside. With these mechanisms, Internet connectivity remains available, while it is no longer possible to identify individual machines from the outside. By using Destination NAT (DNAT), it is still possible to place servers within the protected network/DMZ and make them available for a certain service. In DNAT, only the IP address – not the port – is translated. Typically, the number of externally visible IP addresses is less than the number being hidden behind the NAT router.

DNS (Domain Name System) (also **Domain Name Service**) – Refers to the more user-friendly names, or aliases instead of having to use computer-friendly IP addresses. Name servers take care of the conversion from number to name. Every institution connected to the Internet must operate at least two independent name servers that can give information about its names and numbers. Additionally, there is a name server for every top-level domain that lists all the subordinate name servers of that domain. Thus the Domain Name System represents a distributed hierarchical database. Normally, however, the database is not accessed by the user him-/herself, but by the network application that he/she is presently working with.

DDoS (Distributed Denial of Service) – Attacks are a nefarious extension of DoS attacks because they are designed as a coordinated attack from many sources simultaneously against one or more targets. See also "DoS attacks".

DoS (Denial of Service) attacks – A major concern to the Internet community because they attempt to render target systems inoperable and/or render target networks inaccessible. DoS attacks typically generate a large amount of traffic from a given host or subnet and it's possible for a site to detect such an attack in progress and defend themselves. See also "Distributed DoS attacks".

Encapsulation – The technique used by layered protocols in which a layer adds header information to the protocol data unit (PDU) from the layer above. For example, in Internet terminology, a packet would contain a header from the physical layer, followed by a header from the datalink layer (e.g., Ethernet), followed by a header from the network layer (IP), followed by a header from the transport layer (e.g. TCP), followed by the application protocol data.

Encryption – A form of security wherein readable data is changed to a form that is unreadable to unauthorized users. Encryption involves the conversion of data into a secret code for transmission over a public network. The original (plain) text is converted into coded form (called cipher text) using an encryption algorithm. The cipher text is decoded (decrypted) at the receiving end, and is converted back into plain text.

ESP (Encapsulating Security Payload) – An authentication protocol much like AH. IP ESP may be applied in combination with AH. Security services can be provided between a pair of communicating hosts, between a pair of communicating security gateways, or between a security gateway and a host. ESP may be used to provide the same security services as AH, plus it provides an encryption service. The main difference between the ESP authentication method and the AH authentication method is that ESP does not protect any IP header fields unless those fields are encapsulated by ESP (tunnel mode). ESP is important for the integrity and encryption of datagrams. You can define ESP (and other protocols) for the RouteFinder from **VPN > IPSec**.

Expiration Date – Certificates and keys may have a limited lifetime, and expiration dates are used to monitor and control their useful life.

Filter – A set of rules that define what packets may pass through a network. Filters can use source, destination, or protocol to determine whether to pass or discard a packet transmission. Part of a packet (the header) must contain information that matches the information in the defined rules or else the packet filter will discard it.

Filtering – The act or process of defining which data traffic is to be allowed between the network and hosts, typically using packet filter rules. Filtering is the central part of firewall security. With packet filter rules, you define which data traffic is allowed between the networks and hosts. You can also define particular packets to be filtered and are not to be allowed to pass through the firewall. Several types of filtering exist (e.g., Protocol filtering, port number filtering, URL address filtering, and IP address filtering).

Finger – Windows NT and 2000 have a TCP/IP utility called **Finger**. This utility is an old TCP/IP tool (very popular on UNIX systems) that matches an email address with the person who owns it and provides information about that person. While the Finger utility is fairly old (there are more advanced tools available that perform the same general function), it still works and can be a useful tool in certain situations.
The Finger utility was actually developed as the Finger Information Protocol. Finger was designed to provide an interface to the Remote User Information Program (RUIP). RUIP provides information about users who have accounts on UNIX-based computer networks. The Finger utility was created six years before the Internet was born. The first documentation on the Finger utility was in IETF RFC742, dated December 1977. A popular slogan promoting the phone book's yellow pages was "Let your fingers do the walking". The utility was christened "Finger", since the utility was basically designed for tracking down people.
The Finger Information Protocol let UNIX users on college campuses create a profile, called a "Plan page", which included personal and job-related information. A Plan page was similar to a personal home page on the Internet today. So when someone "Fingered" your email address, they learned more about you. The Finger utility is a command line tool, so in Windows NT or Windows 2000 you must first access a command-prompt window to use it. You then type the command followed by an email address.

Firewall – A device that serves to shield and thus protect a (partial) network (e.g., RouteFinder) from another network (e.g. the Internet). The entire network traffic runs via the firewall where it can be controlled and regulated. Technically this can be achieved in different ways. The use of special hardware firewalls is rare. More frequent is the use of routers with firewall options. The most common is use of firewall software on a specially dedicated computer.

Gateway – A combination of hardware and software that links two different types of networks. E.g., gateways between email systems allow users on different email systems to exchange messages.

Hacker – A person who tries to, and/or succeeds at defeating computer security measures.

Hacking Lexicon – The terms used by hackers; entire dictionaries exist to document hacking terms (e.g., http://www.robertgraham.com/pubs/hacking-dict.html). These documents clarify many of the terms used within the context of information security (infosec).

Hash – A one-way security function that takes an input message of arbitrary length and produces a fixed-length digest. Used in SHA (Secure Hash Algorithm).

Header – The portion of a packet, preceding the actual data, containing source and destination information. It may also error checking and other fields. A header is also the part of an electronic mail message that precedes the body of a message and contains, among other things, the message originator, date and time

Host – In client-server architectures, the computer on which the server software is running is called the host. It is possible for several servers to be running on one host, e.g. one FTP server and one email server. Hosts can be accessed with the help of clients, e.g. with a browser or an email program. As the expression *server* is used for the program (i.e. the software) as well as for the computer on which the program is running (i.e. the hardware), *server* and *host* are not clearly separated in practice. In data telecommunication the computer from which information (such as FTP flies, news, www pages) is fetched, is called the host. A host is also called a node in the Internet. Using an Internet host (as opposed to a local host), it is possible to work from a distance (remote access).

Host – A computer that allows users to communicate with other host computers on a network. Individual users communicate by using application programs, such as electronic mail, Telnet, and FTP.

HTTPS (aka, **S-HTTP)** – Secure HyperText Transfer Protocol, a secure way of transferring information over the World Wide Web. HTTPS refers to the entry (e.g., https://192.168.2.100) used for an S-HTTPS connection. S-HTTPS is the IETF RFC that describes syntax for securing messages sent using the Hypertext Transfer Protocol (HTTP), which forms the basis for the World Wide Web. S-HTTP provides independently applicable security services for transaction confidentiality, authenticity/integrity and non-repudiability of origin. S-HTTP emphasizes maximum flexibility in choice of key management mechanisms, security policies and cryptographic algorithms by supporting option negotiation between parties for each transaction.

ICMP – The **Internet Control Message Protocol** notifies the IP datagrams sender about abnormal events. ICMP might indicate, for example, that an IP datagram cannot reach an intended destination, cannot connect to the requested service, or that the network has dropped a datagram due to old age. ICMP also returns information to the transmitter, such as end-to-end delay for datagram transmission.

IETF (**Internet Engineering Task Force**) – The international standards body that has standardized the IP protocol and most of the other successful protocols used on the Internet. The IETF web page is at http://www.ietf.org/.

IKE (Internet Key Exchange) – A hybrid Internet protocol used to establish a shared security policy and authenticated "keys" for services, such as IPSec, that require keys.

IP – The **Internet Protocol** (IP) is the basic protocol for the transmission of Internet information. It has been in use virtually unchanged since 1974. It establishes and ends connections, as well as recognizing errors. By using NAT and Masquerading, private networks can be mapped onto official IP addresses. This way, the Ipv4 address space will still last a long time. Standard Internet open protocols include:

Protocol	Function
TCP/IP	basic network communication
HTTP	browsing
NFS	File Service
IMAP4/SMTP	Mail Service
DNS	Naming Service
DNS/LDAP	Directory Services
Bootp/DHCP	Booting Services
SNMP	Network Administration

IP Address – A 32-bit number that identifies the devices using the IP protocol. An IP address can be unicast, broadcast, or multicast. See RFC 791 for more information. Every host has a clear IP address, comparable with a telephone number. An IP address consists of four decimal numbers between 1 and 254, divided by dots (e.g., a possible IP address is 212.6.145.0. At least one name of the form xxx belongs to every IP address (e.g. xxx). This defines a computer with the name ox that is in the sub domain xxx of the sub domain xxx of the domain xxx. Like with IP addresses, the individual name parts are divided by dots. However, as opposed to IP addresses, IP names are not limited to four parts. Also, several IP names can be assigned to one IP address; these are referred to as aliases.

IP Header – The part of the IP packet that carries data used on packet routing. The size of this header is 20 bytes, but usually the IP options following this header are also calculated as header. The maximum length of the header is 60 bytes. The header format is defined in RFC 791.

IP Packet – A self-contained independent entity of data carrying sufficient information to be routed from the source to the destination computer without relying on any earlier exchange between this source and destination computer and the transporting network. The Internet Protocol (IP) is defined in RFC 791.

IP Payload – The part of the IP packet that carries upper level application data.

IPSec (IP Security) – A set of IETF standards that provide authentication and encryption for IP-based and Internet-based VPNs.

Key – A data string which, when combined with source data (packet) using a special algorithm, produces output that cannot be read without that specific key. Key data strings are typically 40-168 bits in length.

Key Agreement – A process used by two or more parties to agree upon a secret symmetric key.

Key Exchange – A process used by two more parties to exchange keys in cryptosystems.

Key Generation – The act or process of creating a key.

Key Management – The various processes that deal with the creation, distribution, authentication, and storage of keys.

Key Pair – Full key information in a public-key cryptosystem; consists of the public key and private key.

L2TP (**Layer Two Tunneling Protocol**) – A security protocol that facilitates the tunneling of PPP packets across an intervening network in a way that is highly-transparent to both end-users and applications. L2TP is defined in IETF RFC 2661.

LILO (LInux LOader) – LILO is a small program that sits on the master boot record of a hard drive or on the boot sector of a partition. LILO is used to start the loading process of the Linux kernel. (There are other programs that can also do this, such as **grub**. Most distributions/versions of Linux use LILO.) You can set up lilo to require a password to start to load the Linux kernel, or you can set it up to require a password if you want to pass any extra options to the Linux kernel before it starts loading.

Mapping – Logically associating one set of values (such as addresses on one network) with values or quantities on another set (such as devices on another network). Examples include name-address mapping, inter-network route mapping, and DNAT port mapping. Name resolution (name to address mapping) is another example.

Masquerading – The concealing of internal network information (LAN) form the outside. For example, the computer of a colleague with the IP address is inside a masked network. All the computers inside his network are assigned one single, official IP address (i.e. if he starts an HTTP request into the Internet, his IP address is replaced by the IP address of the external network card). This way, the data packet entering the external network (Internet) contains no internal information. The answer to the request is recognized by the firewall and diverted to the requesting computer.

MD5 (Message Digest 5) – A one-way hashing algorithm that produces a 128-bit hash. It computes a secure, irreversible, cryptographically strong hash value for a document. The MD5 algorithm is documented in IETF RFC 1321.

Message Digests – Mathematical functions (aka, one-way hashes) that are easy to compute but nearly impossible to reverse. The message digest serves as a "fingerprint" for data. As such, it is an element of most data security mechanisms (e.g., Digital Signatures, SSL, etc.). The hashing function takes variable-length data as input, performs a function on it, and generates a fixed-length hash value.

MPPE (Microsoft Point-to-Point Encryption) – An encryption technology developed by Microsoft to encrypt point-to-point links. The PPP connections can be over a VPN tunnel or over a dial-up line. MPPE is a feature of Microsoft's MPPC scheme for compressing PPP packets. The MPPC algorithm was designed to optimize bandwidth utilization in supporting multiple simultaneous connections. MPPE uses the RC4 algorithm, with either 40-bit or 128-bit keys, and all MPPE keys are derived from clear text authentication of the user password. The RouteFinder supports MPPE 40-bit/128-bit encryption.

Name Resolution – The process of mapping a name into its corresponding address.

NAT (Network Address Translation) – IP NAT is comprised of a series of IETF standards covering various implementations of the IP Network Address Translator. NAT translates multiple IP addresses on the private LAN to one public address that is sent out to the Internet. This adds a level of security since the address of a PC connected to the private LAN is never transmitted on the Internet.

Netfilter – The Linux packet filter and network address translation (NAT) system that aims to reduce the number of filter points and to separate the filtering function from the NAT function. Netfilter is derived from the Linux **ipchains** and the Unix **ipfilter** packet filtering systems. The RouteFinder uses a Linux 2.4 kernel (and, for example, **iptables** for the internal logic in the netfilter code).

Network Card – The Ethernet PC card used to connect the RouteFinder to the internal, external or DMZ network (aka: NIC or NIC card).

NIC (**Network Interface Card**) – The Ethernet PC card used to connect the RouteFinder to the internal, external or DMZ network (aka, Network Card).

Nslookup – A Unix program for accessing name servers. The main use is the display of IP names for a given IP address and vice versa. Beyond that, other information can also be displayed (e.g., aliases).

Packet Filter – An operation that blocks traffic based on a defined set of filter "rules" (e.g., IP address or port number filtering).

PCT (**Private Communications Technology**) – A protocol developed by Microsoft that is considered more secure than SSL2. (Note that some web sites may not support the PCT protocol.)

PING (**Packet InterNet Groper**) – A program to test reachability of destinations by sending an ICMP echo request and waiting for a reply. The term is also used as a verb: "Ping host X to see if it is up."

PKI (**Public Key Infrastructure**) – Consists of end entities that possess key pairs, certification authorities, certificate repositories (directories), and all of the other components, software, and entities required when using public key cryptography.

Plaintext – Information (text) which has not been encrypted. (The opposite is ciphertext.)

PFS (**Perfect Forward Secrecy**) – Refers to the notion that any single key being compromised will permit access to only data protected by that single key. In order for PFS to exist, the key used to protect transmission of data must not be used to derive any additional keys. If the key used to protect transmission of data was derived from some other keying material, that material must not be used to derive any more keys. Sometimes referred to as Perfect Secret Forwarding, **PSF** is a security method that ensures that the new key of a key exchange is in no way based on the information of an old key and is therefore unambiguous. If an old key is found or calculated, no conclusions can be drawn about the new key. On the RouteFinder, PFS is configured in **VPN > IPSec**.

Policy – The purpose of an IPSec Security Policy is to define how an organization is going to protect itself. The policy will generally require two parts: a general policy and specific rules
(e.g., a system-specific policy). The general policy sets the overall approach to Security. The rules define what is and what is not allowed. The Security Policy describes how data is protected, which traffic is allowed or denied, and who can and cannot use various network resources.

Port – Where as only the source and target addresses are required for transmission on the IP level, TCP and UDP require further characteristics to be introduced that allow a differentiation of the separate connections between two computers. A connection on the TCP and UDP level are thus clearly identified by the source address and the source port, as well as by the target address and the target port.

Port Range – A series of TCP or UDP port numbers that can be set in RouteFinder protocol service definitions. For example, when adding a service from **Networks & Services > Services**, enter the source (client) port. The entry options are a single port (e.g. 80), a list separated by commas (e.g. 25, 80, 110), or a port range (e.g. 1024:64000).

Port Scanning – Attempting to find "listening" UDP or TCP ports on an IP device, and then obtaining information about the device. Portscanning itself is not harmful, but it can be used by hackers to allow intrusion by brute-force password guessing.

PPP (Point-to-Point Protocol) – An IETF standard which provides a method for transporting multi-protocol datagrams over point-to-point links. All of the users on the Ethernet connection share a common connection, so the Ethernet principles supporting multiple users in a LAN are combined with the principles of PPP, which typically apply t serial connections.

PPPoE (Point-to-Point Protocol over Ethernet) – An IETF standard which provides the ability to connect a network of hosts over a simple bridging access device to a remote access concentrator. To provide a point-to-point connection over Ethernet, each PPP session must learn the Ethernet address of the remote peer, as well as establish a unique session identifier.

PPTP (Point-To-Point Tunneling Protocol) – A protocol that allows secure remote access to corporate networks (VPNs) over the Internet. All data sent over a PPTP connection can be encrypted and compressed, and multiple network level protocols (TCP/IP, IPX) can be run concurrently. **Note**: the RF660VPN does NOT support IPX or Netbeui when using PPTP tunneling.

Protocol – A clearly defined and standardized sentence of commands and answers, with whose help a client and a server can communicate. Well-known protocols and the services they provide are, for example, HTTP (www), FTP (ftp), and NNTP (news).

Proxy (Application Gateway) – The task of a proxy (Application Gateway) is to completely separate the communication connections between the external network (Internet) and the internal network (LAN). There must be no direct connection between an internal system and an external computer. The proxies work exclusively on the application level. Firewalls that are based on proxies use a dual homed gateway that does not transfer any IP packets. The proxies that run as specialized programs on the gateway can now receive connections for a special protocol, process the received information at the application level, and then transfer them.

Proxy ARP – The technique in which one machine, usually a router, answers ARP requests intended for another machine. By "faking" its identity, the router accepts responsibility for routing packets to the "real" destination. Proxy ARP allows a site to use a single IP address with two physical networks. Subnetting would normally be a better solution.

Private Key – In public key cryptography the private key is only known to the holder, and it can be used to sign and decrypt messages.

Proxy – A cache server that acts as a firewall, protecting the local network. It allows an application inside the proxy to access resources on the global Internet.

PSK (Pre Shared Key) – A PSK password must be entered at both ends of the VPN tunnel. This password is also called the secret. The holder of this password can establish a VPN connection to the secure network. Make sure that this password does not reach the wrong hands and that you change the PSK password at regular intervals.

Public Key – In public key cryptography the public key, which is included in the certificate, can be used to verify signatures and encrypt messages. A sample public key is shown below:


```
0sAQNic1Tww7iknvNd6ieKDhd9JTu/Krbc71H4oIFd/xqKJntU8x25M0Wbxr0
gQngECdZPWHj6KeSVtMtslzXMkxDecdawoCadPtPiH/lln23GKUOt3GoDVM
ob+fob9wBYbwdHOxPAYtNQBxNPEU9PGMxQdYp8io72cy0duJNCXkEVvpv
YvVzkmp0xVYOWYkfjiPsdhnz5FCitEh6XsCe0ctByoLjKA1C+mLtAlWhuycVoj
r2JwzSqUlJXzS6nV4yrpI+QY5o5yztgjVlgwW1Er6jyyo2aeFLgucqjuHSZ+sX0
dz/OfdQ0N0AjRAmO3eknOYLk2DPRkmUeYr3W95q1Z2j/+4GRlzzP8ZoyPw
dBv7hpZ0TRA9c38a26+La8N2/TDKx+fGLfixB6Ed8X0jCmq4lt7iD2d/9EWea
UZfctqaKfw==
```


Public key cryptography is based on two keys, a private key and a public key. Where conventional cryptography is a one key system for both locking (encrypting) and unlocking (decrypting) a message, whereas public key cryptography uses different keys for locking and unlocking. In public-key systems, one key can be kept private while the other key is made public. Knowing that the public key does not reveal the private key.

PuTTY – A simple but excellent ***SSH*** and ***Telnet*** replacement for Windows 95/98/NT that happens to be free. Installation is simple - you download ***PuTTY.exe*** and store it somewhere on your system that's convenient.

Qmail – A security-oriented Unix mailer daemon developed by Dan Bernstein.

RADIUS – RADIUS stands for **Remote Authentication Dial-In User Service**. RADIUS is a protocol with which the router can obtain information for the user authentication from a central server.

RFC (**Request For Comments**) – A document of Internet Society under standardization. See also IETF.

RFC 921 – A policy statement on the implementation of the Domain Style Naming System on the Internet. RFC 921 details the schedule for the implementation for the Domain Style Naming System in terms of 1) the names themselves, 2) the method of translating names to addresses, and 3) the relationship between the Internet and the rest of the world.

RFC 953 – The official IETF specification of the Hostname Server Protocol, a TCP-based host information program and protocol. The function of this server is to deliver machine-readable name/address information describing networks, gateways, hosts, and eventually domains, within the Internet environment. To access this server from a program, establish a TCP connection to port 101 (decimal) at the service host, SRI-NIC.ARPA (26.0.0.73 or 10.0.0.51).

RFC 1918 – An IETF standard for Address Allocation for Private Internets.

Rijndael (pronounced *Rhine-doll*) – A security standard for data encryption chosen as the proposed U.S. government AES standard to protect sensitive data and to spur the digital economy, replacing DES. The RouteFinder uses Rijndael in the SSH IPSec client software (refer to Appendix F of this manual).

Router (**Gateway**) – A router is a device that selects intelligent pathways for network packets. Strictly speaking, a gateway is something different than a router, but in connection with TCP/IP, both terms are synonyms. To establish connections throughout world and not just stay within one's own network, one has to introduce this router (gateway) to one's computer. Normally, the highest address on the network 134.93.178.0 is the address 134.93.179.254 (since 134.93.179.255 is the broadcast). Generally, a router is a node that forwards packets not addressed to itself. Requirements for a router are defined in IETF RFC 1812.

RSA – A public key encryption and digital signature algorithm. It was invented by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm was patented by RSA Security, but the patent expired in September 2000.

Rsync – A synchronization protocol that uses checksums to determine differences (as opposed to using modification dates) and does a partial file transfer (transferring only the differences instead of entire files). **Rsync** was developed by Andrew Tridgell and Paul Mackerras; the **rsync** daemon (***rsyncd***) provides an efficient, secure method for making files available to remote sites.

Rules – The configuration settings used to set how packets are filtered. The rules are set with the network and service definitions set up in the **Networks & Services** menu. When setting packet filter rules, the two basic types of security policies are:

1. All packets are allowed through – the rules setup must be informed explicitly what is forbidden.
2. All packets are blocked – the rules setup needs information about which packets to let through. This lets you explicitly define which packets may pass through the filter. All other packets are blocked and can be displayed for viewing. See also "Filtering".

SA (**Security Association**) – A unidirectional connection created for security purposes. All traffic traversing an SA is provided the same security processing. In IPSec, an SA is an Internet layer abstraction implemented via the use of an AH or ESP. It contains data controlling how a transformation is applied to an IP packet. The data is determined using specially defined SA management mechanisms. The data may be the result of an automated SA and key negotiation or it may be defined manually. The SA is defined in IETF RFC 2401.

SCP (Secure copy) – The main purpose of SCP is the safe copying of files between local and remote computers. The RouteFinder supports login using SCP. A Windows SCP client can be downloaded from http://winscp.vse.cz/eng/. WinSCP is freeware SCP client for Windows 95/98/2000/NT using SSH (Secure shell). WinSCP manages some other actions with files beyond the basic file copying function.

Secret Key – The key used both for encryption and decryption in secret-key cryptography.

Secure Channel – A communication medium that is safe from the threat of eavesdroppers.

Seed – A random bit sequence used to generate another, usually longer, pseudo-random bit sequence.

Security Policy – Enterprises should have a carefully planned set of statements in place regarding network protection. A good corporate Internet security policy should define acceptable use, acceptable means of remote access, information types and required encryption levels, firewall hardware and software management processes and procedures, non-standard access guidelines, and a policy for adding new equipment to the network. New security protocols, new services, and security software upgrades should also be considered. The purpose of a security policy is to define how an organization is going to protect itself. The policy will generally require two parts: a general policy and specific rules (system specific policy). The general policy sets the overall approach to security. The rules define what is and what is not allowed. The security policy describes how data is protected, which traffic is allowed or denied, and who is able to use the network resources.

Server – A server is a device on the network that provides mostly standardized services (e.g., www, FTP, news, etc.). To be able to use these services, you as a user require the comparable client requirements for the desired service.

SHA (Secure Hash Algorithm) – A United States government standard for a strong one-way, hash algorithm that produces a 160-bit digest. See MD5. SHA-1 is defined in FIPS PUB 180-1.

SHA-1 (**Secure Hash Algorithm version one**) – The algorithm designed by NSA, and is part of the U.S. Digital Signature Standard (DSS).

S-HTTP (Secure HTTP) – The IETF RFC that describes a syntax for securing messages sent using the Hypertext Transfer Protocol (HTTP), which forms the basis for the World Wide Web.
Secure HTTP (S-HTTP) provides independently applicable security services for transaction confidentiality, authenticity/integrity and non-repudiability of origin. The protocol emphasizes maximum flexibility in choice of key management mechanisms, security policies, and cryptographic algorithms by supporting option negotiation between parties for each transaction. The current IETF RFC describes S-HTTP version 1.2. Previous versions of S-HTTP numbered 1.0 and 1.1 have also been released as Internet-Drafts.

SNAT (Source NAT) – A functionality equivalent to DNAT, except that the source addresses of the IP packets are converted instead of the target address. This can be helpful in more complex situations (e.g., for diverting reply packets of connections to other networks or hosts). In contrast to Masquerading, SNAT is a static address conversion, and the rewritten source address does not need to be one of the firewall's IP addresses. To create simple connections from private networks to the Internet, you should use the Masquerading function instead of SNAT.
The use of private IP addresses in combination with Network Address Translation (NAT) in the form of Masquerading, Source NAT (SNAT), and Destination NAT (DNAT) allows a whole network to hide behind one or a few IP addresses preventing the identification of your network topology from the outside. With these mechanisms, Internet connectivity remains available, while it is no longer possible to identify individual machines from the outside. Using DNAT makes it possible to place servers within the protected network/DMZ and still make them available for a certain service.

SOCKS – A proxy protocol that allows the user to establish a point-to-point connection between the own network and an external computer via the Internet. Socks, also called Firewall Transversal Protocol, currently exists at version 5.

SPI (Security Parameters Index) – The SPI is an arbitrary 32-bit value that, in combination with the destination IP address and security protocol (AH), uniquely identifies the Security Association for a datagram. SPI values from 1 through 255 are reserved by the Internet Assigned Numbers Authority (IANA) for future use; a reserved SPI value will not normally be assigned by IANA unless the use of the assigned SPI value is specified in an RFC. It is ordinarily selected by the destination system upon establishment of an SA. You can define SPI (and other protocols) for the RouteFinder from **VPN > IPSEC**. SPI is defined in RFC 2401.
SSH (Secure Shell) is a text-oriented interface to a firewall, suitable only for experienced administrators. The SSH is a secure remote login program available for both Unix and Windows NT. For access via SSH you need an SSH Client, included in most Linux distributions. The Microsoft Windows program PuTTY is recommended as an SSH client. Access via SSH is encrypted and therefore impossible for strangers to tap into.

Stateful Inspection – A method of security that requires a firewall to control and track the flow of communication it receives and sends, and to make TCP/IP-based services decisions (e.g., if it should accept, reject, authenticate, encrypt and/or log communication attempts). To provide the highest security level possible, these decisions must be based on the Application State and/or the Communication State (as opposed to making decisions based on isolated packets). With stateful inspection, a firewall is able to obtain, store, retrieve, and manipulate information it receives from all communication layers as well as from other applications. Stateful inspection tracks a transaction and verifies that the destination of an inbound packet matches the source of a previous outbound request. Other firewall technologies (e.g., packet filters or application layer gateways) alone may not provide the same level of security as with stateful inspection.

Static Route – A directive in a node that tells it to use a certain router or gateway to reach a given IP subnet. The simplest and most common example is the default router/gateway entry entered onto any IP-connected node (i.e., a static route telling the node to go to the Internet router for all subnets outside of the local subnet).

Subnet Mask – The subnet mask or the net mask indicates into which groups the addresses are divided. Based on this arrangement, individual computers are assigned to a network.

S/WAN – Secure Wide Area Network is a Linux implementation of IPSEC and IKE for Linux. At the RouteFinder's **VPN > IPSec > Add an IKE connection > RSASig > Generate** function, the imported key must meet S/WAN requirements.

Syslog – A service run mostly on Unix and Linux systems (but is also available for most other OSes) to track events that occur on the system. Other devices on the network may also be configured to use a given node's syslog server to keep a central log of what each device is doing. Analysis can often be performed on these logs using available software to create reports detailing various aspects of the system and/or the network.

TCP (**Transmission Control Protocol**) – A widely used connection-oriented, reliable (but insecure) communications protocol; the standard transport protocol used on the Internet. TCP is defined in IETF RFC 793.

Telnet – The Internet standard protocol for remote terminal connection service. It is defined in IETF RFC 854 and extended with options by many other RFCs.

TLS (**Transport Layer Security**) – An open security standard that is similar to SSL3. (Note that some web sites may not support the TLS protocol.)

Trace Route – A program available on many systems that traces the path a packet takes to a destination. It is mostly used to debug routing problems between hosts. A Trace Route protocol is defined in IETF RFC 1393.

Trusted Subnetwork – A subnetwork of hosts and routers that can trust each other not to engage in active or passive attacks. It is also assumed that the underlying communications channel such as a LAN is not being attacked by any other means.

Tunneling – Transmitting data that is structured in one protocol within the protocol or format of a different protocol.

UDP (User Datagram Protocol) – A datagram-oriented unreliable communications protocol widely used on the Internet. It is a layer over the IP protocol. UDP is defined in IETF RFC 768.

UNC (Universal Naming Convention) path – A UNC path (e.g., \\server) is used to help establish a link to a network drive.

URL (**Universal Resource Locator**) – URLs are used to describe the location of web pages, and are also used in many other contexts. An example of an URL is http://www.ssh.com/ipsec/index.html. URLs are defined in IETF RFCs 1738 and 1808.

Verification – The act of recognizing that a person or entity is who or what it claims to be.

VLAN (Virtual Local Area Network) – A function allowing some Ethernet switches to be divided into smaller logical groups known as VLANs. On most switches each VLAN operates completely independent of the others, as if each was a separate physical device. Some higher-end switches can also route between VLANs as if each was a separate hub/switch connected by a router.

VPN (Virtual Private Network) – A device or program that protects users and their data when exchanging information over the Internet. A VPN can use encryption, user authentication, and/or firewall protection to solve remote access security threats.

WAN (Wide Area Network) – A data network, typically extending a LAN beyond a building or campus, linking to other (remote) LANs.

Index

T

U

V

W

X